REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

A TEORIA DA PROFUNDIDADE ESTRATÉGICA CIBERNÉTICA: SOBERANIA, RESILIÊNCIA E PODER NACIONAL NA ERA INFORMACIONAL

THE THEORY OF CYBER STRATEGIC DEPTH: SOVEREIGNTY, RESILIENCE, AND NATIONAL POWER IN THE INFORMATION AGE

Ciências Humanas, Ciências Sociais Aplicadas • 24/06/2026

REGISTRO DOI: 10.70773/revistatopicos/782277603

Wanderlino Moreno Junior[1]

RESUMO

A transformação digital das sociedades produziu mudanças estruturais nos fundamentos clássicos da soberania, da segurança e do poder estatal. Embora a literatura geopolítica tenha consolidado o conceito de profundidade estratégica como elemento associado à dimensão territorial dos Estados, ainda não existe um modelo teórico capaz de explicar como eles constroem profundidade estratégica em ambientes digitais altamente interconectados. O presente artigo propõe a Teoria da Profundidade Estratégica Cibernética (TPEC), concebida como uma ampliação da teoria clássica da profundidade estratégica para a Era Informacional. O estudo tem caráter qualitativo, de natureza exploratório-explicativa, por meio de revisão sistemática da literatura, baseada no protocolo PRISMA 2020, método hipotético-dedutivo e estudo de caso, aplicado ao ecossistema PIX brasileiro. Argumenta-se que a sobrevivência estratégica dos Estados depende da capacidade de construir profundidade nas camadas física, lógica e cognitiva do espaço cibernético, reduzindo simultaneamente sua dependência tecnológica externa. Como contribuição original, o artigo propõe o Índice de Profundidade Estratégica Cibernética (IPEC), destinado à mensuração comparativa da capacidade de resiliência informacional dos Estados. Os resultados sugerem que a profundidade estratégica contemporânea não é determinada exclusivamente pela extensão territorial, mas pela capacidade de absorver, resistir e recuperar-se de ameaças dirigidas ao ecossistema informacional nacional. Conclui-se que ela constitui uma nova projeção do Poder Nacional e um dos principais fundamentos da soberania no século XXI.

Palavras-chave: Profundidade Estratégica Cibernética; Soberania Cibernética; Poder Nacional; Geopolítica Digital; Resiliência Nacional; Segurança Cibernética.

ABSTRACT

The digital transformation of societies has produced structural changes in the classic foundations of sovereignty, security, and state power. Although geopolitical literature has consolidated the concept of strategic depth as an element associated with the territorial dimension of states, there is still no theoretical model capable of explaining how they build strategic depth in highly interconnected digital environments. This article proposes the Theory of Cybernetic Strategic Depth (TSD), conceived as an extension of the classic theory of strategic depth for the Information Age. The study is qualitative, exploratory-explanatory in nature, through a systematic literature review based on the PRISMA 2020 protocol, a hypothetical-deductive method, and a case study applied to the Brazilian PIX ecosystem. It is argued that the strategic survival of states depends on the ability to build depth in the physical, logical, and cognitive layers of cyberspace, simultaneously reducing their external technological dependence. As an original contribution, this article proposes the Cyber Strategic Depth Index (CSD), designed for the comparative measurement of the informational resilience capacity of States. The results suggest that contemporary strategic depth is not determined exclusively by territorial extent, but by the capacity to absorb, resist, and recover from threats directed at the national informational ecosystem. It is concluded that it constitutes a new projection of National Power and one of the main foundations of sovereignty in the 21st century.

Keywords: Cyber Strategic Depth; Cyber Sovereignty; National Power; Digital Geopolitics; National Resilience; Cybersecurity.

1. INTRODUÇÃO

As transformações tecnológicas ocorridas nas últimas décadas provocaram uma das mais profundas mudanças na história da organização política, econômica e social da humanidade. A digitalização das atividades produtivas, a expansão das redes globais de comunicação, o surgimento das plataformas digitais e o avanço da inteligência artificial alteraram significativamente os mecanismos tradicionais de exercício do poder e da soberania.

Historicamente, a capacidade de sobrevivência dos Estados esteve associada ao controle dos espaços geográficos. A geografia funcionava simultaneamente como recurso estratégico e mecanismo de proteção. As montanhas, os desertos, oceanos e selvas ampliavam a capacidade de resistência diante de ameaças externas. Nesse contexto, a profundidade estratégica consolidou-se como um dos conceitos centrais da Geopolítica e dos Estudos Estratégicos.

Ela é compreendida, em sua acepção clássica, como a capacidade de um Estado absorver ameaças por meio da distância geográfica existente entre suas fronteiras e seus centros vitais de poder. Quanto maior essa distância, maior o tempo disponível para mobilização de recursos, reorganização das forças nacionais e preservação da capacidade de resistência.

A história oferece inúmeros exemplos da relevância desse conceito. A Rússia resistiu às invasões napoleônicas e alemãs em grande medida graças à sua profundidade territorial. Os Estados Unidos beneficiaram-se da proteção oferecida pelos oceanos Atlântico e Pacífico. O Reino Unido utilizou sua condição insular para preservar sua segurança diante de sucessivas ameaças continentais. Em todos

esses casos, a geografia constituiu elemento fundamental da sobrevivência estratégica.

Entretanto, a consolidação da Era Informacional alterou profundamente essa lógica. A crescente dependência das infraestruturas digitais produziu um cenário no qual a distância geográfica perdeu parte significativa de sua relevância estratégica. Um ataque cibernético conduzido a milhares de quilômetros de distância pode produzir efeitos imediatos sobre sistemas financeiros, redes energéticas, telecomunicações, estruturas governamentais e infraestruturas militares. O fator distância, historicamente associado à proteção estratégica, tornou-se menos relevante diante da velocidade dos fluxos informacionais.

Ao mesmo tempo, novos ativos estratégicos passaram a ocupar posição central nas relações internacionais. Os dados, algoritmos, sistemas de inteligência artificial, data centers, redes digitais e plataformas tecnológicas tornaram-se recursos fundamentais para a produção de riqueza, exercício do poder e preservação da soberania.

Essa transformação produziu uma mudança estrutural na natureza das vulnerabilidades estatais.

Se durante grande parte da história as ameaças eram predominantemente direcionadas ao território físico, no século XXI elas passaram a incidir crescentemente sobre infraestruturas digitais, sistemas de informação e percepções coletivas. Os ataques cibernéticos, as campanhas de desinformação, a espionagem digital, a manipulação algorítmica e a dependência tecnológica passaram a constituir desafios centrais para a autonomia e independência dos Estados.

Assim, se coloca um problema central: como conseguir que os Estados preservem sua independência estratégica numa área caracterizada pela crescente dependência digital e pela redução da relevância da distância geográfica?

A literatura contemporânea oferece respostas parciais para essa questão. Os estudos sobre Poder Cibernético analisam a projeção de poder no domínio cibernético. As teorias de Soberania Digital discutem a capacidade de governança dos fluxos informacionais. Os modelos de Resiliência Nacional investigam mecanismos de adaptação diante de crises complexas. A literatura sobre Soberania Cibernética examina a autonomia estatal nas camadas física, lógica e cognitiva do ciberespaço.

Todavia, permanece ausente um modelo capaz de explicar como os Estados constroem profundidade estratégica em seus ecossistemas cibernéticos.

Essa lacuna torna-se particularmente relevante diante da crescente dependência das sociedades contemporâneas dos sistemas digitais. A interrupção de plataformas financeiras, sistemas energéticos, redes de comunicação ou infraestruturas governamentais pode produzir impactos equivalentes ou superiores aos observados em conflitos convencionais.

Partindo dessa constatação, o artigo propõe a Teoria da Profundidade Estratégica Cibernética (TPEC). Afirma que a sobrevivência estratégica dos Estados na Era Informacional passa pela capacidade de construir profundidade nas camadas física, lógica e cognitiva do espaço cibernético, reduzindo ao mesmo tempo a sua dependência tecnológica externa.

Em outras palavras, a profundidade estratégica contemporânea não é medida, apenas, pela extensão territorial, mas pela existência de camadas sucessivas de proteção, redundância, autonomia e resiliência capazes de preservar a continuidade do Poder Nacional diante de ameaças dirigidas ao ecossistema cibernético.

A hipótese central da pesquisa afirma que a sobrevivência estratégica dos Estados depende mais da profundidade existente em seus ecossistemas cibernéticos do que da profundidade territorial clássica.

O artigo emprega a revisão sistemática da literatura, o método hipotético-dedutivo, *process tracing* e um estudo de caso aplicado ao ecossistema PIX brasileiro, complementado por uma análise comparativa internacional envolvendo Estados Unidos, China, Estônia e União Europeia.

A sua principal contribuição consiste na formulação de uma nova categoria analítica destinada à compreensão da soberania e da sobrevivência estratégica dos Estados na Era Informacional. Além disso, propõe-se o Índice de Profundidade Estratégica Cibernética (IPEC), concebido como instrumento destinado à mensuração comparativa da capacidade de resiliência informacional dos Estados.

O artigo está estruturado em nove seções. Após esta introdução, apresenta-se a revisão sistemática da literatura. Em seguida são discutidos os fundamentos teóricos da profundidade estratégica informacional, a metodologia empregada, o modelo analítico da teoria, a construção do IPEC, o estudo de caso brasileiro, a validação comparativa internacional e as conclusões.

2. REVISÃO SISTEMÁTICA DA LITERATURA

2.1. Procedimentos Metodológicos da Revisão

Realizou-se uma revisão sistemática da literatura com o objetivo de identificar os principais conceitos, abordagens teóricas e lacunas existentes no campo dos Estudos Estratégicos, Geopolítica, Cibernética e das Relações Internacionais relacionados à sobrevivência estratégica dos Estados na Era Informacional.

A revisão foi conduzida com base nas diretrizes do protocolo PRISMA 2020 (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), amplamente utilizado para garantir transparência, rastreabilidade e rigor metodológico em pesquisas de revisão.

Explorou-se as bases de dados *Scopus, Web of Science*, *JSTOR*, *Science Direct*, *Springer Link*, *Taylor & Francis Online, Wiley Online Library* e *Google Scholar*.

Os descritores utilizados incluíram os termos: *"Strategic Depth", "Strategic Resilience", "Cyber Sovereignty", "Digital Sovereignty", "Cyber Power", "National Resilience", "Cybersecurity Governance", "Information Sovereignty", "Digital Geopolitics" e "Cyber Strategy".*

O período analisado compreendeu os anos de 2000 a 2025, abrangendo a fase de consolidação do ciberespaço como domínio estratégico e a emergência dos debates contemporâneos sobre soberania cibernética, soberania digital e competição tecnológica internacional.

Após a remoção de registros duplicados e a aplicação dos critérios de elegibilidade, os trabalhos selecionados foram agrupados em cinco grandes correntes analíticas: Geopolítica Clássica e

Profundidade Estratégica; Resiliência Nacional; Poder Cibernético; Soberania Digital; e Soberania Cibernética.

Os resultados revelaram significativa produção científica sobre poder, soberania e segurança no ambiente cibernético. Entretanto, não foi identificada uma estrutura teórica especificamente voltada à compreensão da profundidade estratégica em ecossistemas cibernéticos.

Essa constatação fundamenta a proposta da Teoria da Profundidade Estratégica Cibernética.

2.2. A Profundidade Estratégica na Geopolítica Clássica

O conceito de profundidade estratégica possui raízes profundas na tradição geopolítica. Embora nem sempre explicitamente denominado dessa forma, sua lógica esteve presente nos principais autores clássicos da disciplina.

Halford Mackinder, ao formular a teoria do Heartland, associou a capacidade de projeção de poder ao controle do espaço terrestre euroasiático. Sua análise partia do pressuposto de que a geografia constituía fator permanente das relações internacionais e que a extensão territorial poderia oferecer vantagens decisivas para a sobrevivência dos Estados.

Alfred Thayer Mahan, por sua vez, enfatizou o papel do poder marítimo e da capacidade de controlar rotas oceânicas estratégicas. Embora seu foco estivesse voltado para o domínio dos mares, a lógica subjacente permanecia relacionada à criação de profundidade estratégica por meio do controle de espaços geográficos.

Nicholas Spykman complementou essa perspectiva ao defender a importância do Rimland como zona de contenção e projeção de poder. Em sua visão, a sobrevivência estatal dependia da capacidade de controlar áreas estratégicas que permitissem limitar a ação de potenciais adversários.

Posteriormente, Colin Gray aprofundou a relação entre geografia e estratégia ao afirmar que a localização territorial continua sendo elemento determinante do poder, mesmo diante das transformações tecnológicas.

Apesar das diferenças existentes entre esses autores, observa-se um elemento comum: a associação da profundidade estratégica à dimensão espacial do poder.

Nessa perspectiva, a sobrevivência dos Estados depende da existência de espaço físico suficiente para absorver ameaças, preservar recursos e manter a continuidade das operações nacionais.

A transformação digital, entretanto, desafia esse pressuposto. O desenvolvimento das tecnologias reduziu drasticamente os efeitos protetivos da distância geográfica. Os sistemas financeiros, infraestruturas energéticas, telecomunicações e redes governamentais podem ser afetados por agentes localizados em qualquer parte do planeta.

Dessa forma, a profundidade estratégica territorial permanece relevante, mas torna-se insuficiente para explicar a realidade contemporânea.

2.3. A Resiliência Nacional e a Sobrevivência Estatal

O aumento da complexidade dos riscos globais levou diversos autores a investigar a capacidade dos Estados de absorver choques, adaptar-se às crises e recuperar suas funções essenciais.

Estudiosos como Boin, Comfort, Linkov e Wildavsky argumentam que a sobrevivência dos sistemas complexos depende menos da capacidade de evitar crises e mais da habilidade de responder a elas de forma eficiente.

A literatura sobre resiliência nacional expandiu-se significativamente após os atentados de 11 de setembro de 2001 e ganhou novo impulso com a crescente preocupação em relação às ameaças cibernéticas.

Nessa perspectiva, ela é entendida como a capacidade de um sistema continuar operando mesmo sob condições adversas. A abordagem oferece contribuições importantes para a compreensão da segurança contemporânea, especialmente ao enfatizar a adaptação, recuperação e continuidade operacional.

Entretanto, a literatura sobre resiliência nacional apresenta limitações relevantes. Embora explique como os Estados respondem aos choques, ela não oferece um modelo capaz de apresentar como a profundidade estratégica é construída previamente à ocorrência dessas crises.

Em outras palavras, a resiliência descreve a capacidade de reação, mas não necessariamente a estrutura estratégica que torna essa atitude possível. Essa lacuna torna-se particularmente relevante quando analisada à luz da crescente dependência digital dos Estados.

2.4. O Poder Cibernético e a Competição Internacional

O surgimento do ciberespaço como domínio estratégico levou diversos autores a investigar a forma pela qual o poder é exercido nesses ambientes.

Joseph Nye foi um dos primeiros estudiosos a argumentar que o espaço cibernético constitui um novo ambiente de disputa política e estratégica. Em sua interpretação, o poder cibernético corresponde à capacidade de utilizar recursos relacionados à informação para produzir efeitos desejados.

Martin Libicki aprofundou essa discussão ao analisar os impactos militares e estratégicos da guerra cibernética. Sua obra destacou a capacidade dos ataques digitais de produzir efeitos significativos sem a necessidade de confronto físico direto.

Clarke e Knake enfatizaram os riscos associados à crescente dependência de infraestruturas digitais, argumentando que o espaço cibernético se tornou elemento central da segurança nacional contemporânea.

A literatura sobre o poder cibernético oferece importantes contribuições para a compreensão da competição estratégica internacional. Todavia, sua atenção continua predominantemente voltada para a projeção de poder e para as capacidades ofensivas e defensivas dos Estados.

Pouca atenção é dedicada à construção da profundidade estratégica como mecanismo de preservação da autonomia e independência nacional.

2.5. A Soberania Digital e a Governança Tecnológica

O crescimento da influência exercida por grandes empresas de tecnologia levou diversos autores a questionar a capacidade dos Estados de governar os fluxos informacionais que atravessam seus territórios.

Floridi argumenta que a transformação digital produziu novas formas de dependência tecnológica capazes de limitar a autonomia estatal.

Mueller observa que a governança da Internet se tornou espaço de disputa entre Estados, corporações e organizações internacionais.

Neste contexto, a União Europeia desenvolveu uma das abordagens mais influentes sobre soberania digital ao enfatizar a proteção de dados, autonomia tecnológica e regulação das plataformas digitais.

O conceito tornou-se particularmente relevante diante da crescente concentração de recursos digitais em um pequeno número de empresas e países.

Apesar de suas contribuições, a literatura sobre soberania digital concentra-se prioritariamente na governança tecnológica e na autonomia regulatória. A questão da profundidade estratégica permanece relativamente marginal.

2.6. A Soberania Cibernética e as Camadas do Espaço Cibernético

Essa abordagem parte do reconhecimento de que a soberania estatal precisa ser reinterpretada diante da emergência do ciberespaço.

A literatura contemporânea passou a compreender o espaço cibernético como estrutura composta por múltiplas camadas interdependentes.

A camada física compreende infraestruturas críticas, centros de dados, redes de telecomunicações e recursos materiais. A lógica envolve softwares, protocolos, algoritmos e sistemas responsáveis pelo funcionamento das redes. A camada cognitiva refere-se aos usuários, às percepções, aos comportamentos e processos de formação de opinião.

Assim, a soberania cibernética é frequentemente entendida como a capacidade de exercer controle relativo sobre essas três camadas.

Essa abordagem representa importante avanço teórico porque reconhece que a autonomia estatal depende simultaneamente de fatores tecnológicos, econômicos e sociais. Entretanto, mesmo essa corrente não oferece uma explicação sistemática sobre como os Estados constroem profundidade estratégica em cada uma dessas camadas.

Em outras palavras, a soberania cibernética explica a autonomia; não explica necessariamente os mecanismos que garantem sua sobrevivência diante de ameaças persistentes.

2.7. A Lacuna Científica e a Necessidade de Uma Nova Teoria

A análise das cinco correntes identificadas permite observar um padrão recorrente. A Geopolítica Clássica explica a profundidade estratégica territorial. A literatura sobre resiliência nacional explica a capacidade de recuperação diante de crises. Os estudos sobre Poder Cibernético explicam a projeção de poder em ambientes digitais. A

Soberania Digital explica a autonomia tecnológica. A Soberania Cibernética explica o controle estatal sobre as camadas física, lógica e cognitiva do espaço cibernético. Entretanto, nenhuma delas responde de forma satisfatória à seguinte questão:

Como os Estados constroem profundidade estratégica em ecossistemas cibernéticos altamente dependentes de tecnologia, conectividade e fluxos de dados?

Falta que constitui a principal lacuna científica identificada pela presente pesquisa.

Assim, a Teoria da Profundidade Estratégica Cibernética surge precisamente para preencher esse vazio analítico. Sua proposta consiste em ampliar o conceito clássico de profundidade estratégica para além da dimensão territorial, incorporando as camadas física, lógica e cognitiva do espaço cibernético.

A hipótese fundamental é que a sobrevivência estratégica dos Estados na Era Informacional depende da capacidade de construir profundidade nessas camadas, reduzindo simultaneamente a dependência tecnológica externa.

Essa formulação permite estabelecer uma ponte conceitual entre a Geopolítica, os Estudos Estratégicos, a Resiliência Nacional, o Poder Cibernético e a Soberania Cibernética, oferecendo uma nova estrutura analítica para compreender a competição internacional no século XXI.

3. REFERENCIAL TEÓRICO

3.1. O Poder Nacional e as Transformações da Soberania no Século XXI

O conceito de Poder Nacional constitui um dos fundamentos centrais dos Estudos Estratégicos. Tradicionalmente, o poder foi compreendido como a capacidade de uma coletividade política alcançar e manter seus objetivos nacionais, mobilizando recursos materiais e imateriais disponíveis em determinado contexto histórico.

Ao longo do século XX, diferentes escolas de pensamento procuraram identificar os elementos constitutivos do poder estatal. Embora existam variações metodológicas, observa-se amplo consenso quanto ao caráter multidimensional do Poder Nacional, envolvendo componentes políticos, econômicos, militares, psicossociais e científico-tecnológicos.

Observa-se que a ascensão da Era Informacional produziu profundas transformações em todas essas dimensões.

A expressão política passou a depender crescentemente de plataformas digitais, sistemas de comunicação instantânea e mecanismos de influência algorítmica. A expressão econômica tornou-se fortemente vinculada aos fluxos de dados, aos mercados digitais e às infraestruturas tecnológicas globais. A expressão militar passou a incorporar capacidades cibernéticas, inteligência artificial, sistemas autônomos e operações informacionais. A expressão psicossocial tornou-se diretamente influenciada pelas redes sociais digitais, pela circulação de informações e pelos processos de formação de opinião mediados por algoritmos. A expressão científico-tecnológica converteu-se em fator determinante da

competitividade internacional, especialmente diante da corrida global por inteligência artificial, computação quântica, semicondutores e tecnologias disruptivas.

Nesse contexto, o ambiente informacional emerge como dimensão transversal do Poder Nacional.

A informação deixa de constituir apenas um recurso de apoio e passa a ocupar posição central na produção de riqueza, no exercício da autoridade política, na projeção militar e na construção da legitimidade estatal.

Como consequência, a própria noção de soberania sofre um processo de transformação. Historicamente, ela foi associada ao controle territorial e ao monopólio legítimo da autoridade política dentro de fronteiras definidas. A lógica westfaliana (1648) pressupunha relativa coincidência entre espaço político, território e autoridade.

A digitalização da sociedade alterou essa concepção. As plataformas digitais operam simultaneamente em múltiplas jurisdições. Os fluxos informacionais atravessam fronteiras sem restrições físicas. As empresas transnacionais passaram a exercer influência comparável à de muitos Estados, e as infraestruturas críticas nacionais passaram a depender de cadeias complexas globais de suprimentos tecnológicos.

A soberania contemporânea passa a envolver não apenas o controle do território físico, mas também a capacidade de governar fluxos informacionais, proteger infraestruturas digitais e preservar a autonomia decisória diante de dependências tecnológicas externas.

3.2. O Espaço Cibernético Como Domínio Estratégico

O reconhecimento do espaço cibernético como domínio estratégico representa uma das mais importantes mudanças conceituais das últimas décadas. Inicialmente concebido como ambiente destinado ao compartilhamento de informações e à comunicação acadêmica, ele evoluiu para tornar-se uma infraestrutura essencial ao funcionamento das sociedades contemporâneas.

Essa crescente dependência produziu uma alteração significativa na natureza do poder. Ao contrário dos domínios tradicionais — terrestre, marítimo, aéreo e sideral — o ciberespaço caracteriza-se pela falta de uma governança efetiva, escasso debate público, elevado grau de controle privado, constante dependência por inovação, elevada demanda por insumos complexos, a interdependência econômica e de infraestruturas, a constante conectividade, a ausência de fronteiras, o elevado consumo energético, a transversalidade, a convergência em nós e a facilidade de anonimização. Esse conjunto de aspectos o torna um ambiente volátil, inseguro, complexo e ambíguo, com potencial para promover constantes atritos entre os múltiplos atores pela disputa por poder.

Cabe ressaltar que essa configuração reduz parcialmente as vantagens tradicionalmente associadas à geografia. A distância física deixa de constituir barreira efetiva para a projeção de poder. Um agente localizado em qualquer parte do mundo pode comprometer sistemas estratégicos de outro Estado sem atravessar as fronteiras físicas ou empregar meios militares convencionais.

Assim, o controle do território físico já não é suficiente para garantir a autonomia estratégica, tornando-se necessário controlar ou

influenciar os elementos que sustentam o funcionamento do ecossistema informacional nacional.

3.3. A Soberania Cibernética e as Camadas da Autonomia Estatal

A literatura contemporânea sobre soberania cibernética busca responder precisamente a esse desafio da Era Informacional. A partir dessa perspectiva, ela é compreendida como a capacidade de um Estado em exercer o controle sobre as camadas que constituem o espaço cibernético, conforme sugerido por Deibert (2002).

Na visão de Moreno (2026), ela representa a capacidade do Estado de atuar, com autonomia e independência, nas camadas que compõem o espaço cibernético, gerando efeitos intra e extra ciberespaço, de maneira sinérgica com as demais projeções da soberania estatal, assegurando a proteção de seus interesses nacionais, a promoção de sua defesa e segurança e a preservação de sua liberdade decisória frente às influências adversas.

A Teoria dos Conjuntos (Georg Cantor e Richard Dedekind,1870), ampara que ela seja equivalente à soma da soberania cibernética na camada cognitiva, física e lógica.

Nesta ótica, a soberania cibernética cognitiva se manifesta na disputa pela consciência coletiva e no controle da informação. O Estado projeta a sua capacidade de proteger, regular e influenciar a criação de narrativas que sustentam sua legitimidade política, sua coesão social e sua autonomia cultural.

Em relação à soberania cibernética física, ela possui maior concretude na aplicação da autonomia e independência do poder estatal, na medida em que tem por essência o controle e a proteção

dos ativos físicos que promovem o suporte ao espaço cibernético. Tal afirmação é comprovada, em parte, por Mueller (2017), ao defender que a localização física de servidores determina a jurisdição aplicável e, com ela, o alcance da soberania estatal sobre fluxos digitais.

Ao se abordar a soberania cibernética lógica, a falta de concretude atinge relevância. É nesta camada que são identificados os conjuntos de protocolos, sistemas de endereçamento, nomenclaturas de domínios, programas e normas técnicas que possibilitam a comunicação e interação entre as redes digitais. Ela se manifesta pela possibilidade de os Estados moldarem, regulamentarem e, em certas situações, dominarem os sistemas lógicos que garantem a interconectividade. As suas consequências geopolíticas são latentes, na proporção em que os protocolos definem as condições de interoperabilidade e podem favorecer determinados modelos econômicos e políticos em detrimento de outros.

Desta forma, a soberania cibernética é a extensão da soberania clássica ao ambiente digital, em consonância com a soberania terrestre, marítima, aérea e espacial, mas mantendo peculiaridades que advêm do caráter globalizado e da impossibilidade de estabelecer limites rígidos.

Conhecer suas camadas é conhecer onde estão os pontos fortes e fracos, bem como as ameaças e as oportunidades que organizam a sociedade informacional.

Em suma, os Estados excessivamente dependentes de infraestruturas externas tornam-se vulneráveis a interrupções, sanções e pressões geopolíticas. A dependência de soluções

tecnológicas estrangeiras pode limitar significativamente a sua liberdade de ação. Nota-se que, na Era Informacional, controlar narrativas pode ser tão estratégico quanto manter os territórios.

Assim, a contribuição fundamental da teoria da soberania cibernética consiste em demonstrar que a autonomia estatal depende simultaneamente dessas três camadas.

3.4. A Amazônia Cibernética Como Patrimônio Estratégico Nacional

A teoria da Amazônia Cibernética, oferece importante contribuição para a compreensão da dimensão estratégica do ambiente informacional.

Inspirada na analogia com a Amazônia física e com o conceito da Amazônia Azul formulado pela Marinha do Brasil (2004), essa abordagem sustenta que o país possui um patrimônio estratégico informacional cuja proteção é fundamental para a preservação da soberania nacional.

Essa riqueza é composta por: dados; infraestruturas digitais; capacidades científicas; sistemas de inteligência artificial; recursos computacionais; conhecimento tecnológico; capital humano especializado; etc.

A Amazônia Cibernética representa, portanto, o conjunto de ativos informacionais considerados essenciais para o desenvolvimento e a autonomia do Estado brasileiro. Tal como ocorre com a Amazônia física, a simples existência desse patrimônio não garante sua proteção.

A preservação de recursos estratégicos exige capacidade de vigilância, presença estatal, governança e mecanismos de defesa.

Assim, a teoria da Amazônia Cibernética contribui para identificar aquilo que precisa ser protegido. Todavia, não explica integralmente como essa proteção é construída. Em outras palavras, ela define o objeto estratégico, mas não necessariamente os mecanismos que asseguram sua sobrevivência.

Essa limitação abre espaço para o desenvolvimento da Teoria da Profundidade Estratégica Cibernética.

3.5. A Necessidade de Uma Teoria da Profundidade Estratégica Cibernética

Neste ponto, pode-se inferir que a Geopolítica Clássica explica a relação entre poder e território. A teoria da Soberania Cibernética explica a autonomia estatal sobre as camadas física, lógica e cognitiva do espaço cibernético. A teoria da Amazônia Cibernética identifica os ativos informacionais estratégicos que devem ser protegidos. Entretanto, permanece ausente uma teoria capaz de explicar como os Estados constroem capacidade de sobrevivência estratégica em ambientes cibernéticos.

A presente pesquisa sustenta que essa lacuna pode ser preenchida por meio do conceito de Profundidade Estratégica Cibernética.

Se a profundidade estratégica clássica era medida pela distância física existente entre as fronteiras e os centros vitais do Estado, a profundidade estratégica cibernética deve ser compreendida como a distância funcional existente entre uma ameaça digital e a sua capacidade de produzir danos irreversíveis ao sistema nacional.

Essa distância funcional é construída por meio de sucessivas camadas de proteção, redundância, resiliência e autonomia. Assim, quanto maior a capacidade de um Estado em absorver, resistir e recuperar-se de ameaças dirigidas ao seu ecossistema cibernético, maior será sua profundidade estratégica nessa área.

Dessa forma, a teoria proposta não substitui os conceitos anteriores. Ao contrário, atua como elemento integrador.

Essa postura constitui o fundamento conceitual da teoria desenvolvida neste estudo e prepara o caminho para a apresentação do modelo analítico e da metodologia de validação empírica.

4. METODOLOGIA

4.1. O Delineamento da Pesquisa

A presente investigação possui natureza aplicada, com uma abordagem predominantemente qualitativa e caráter exploratório-explicativo. Seu objetivo consiste em desenvolver uma nova estrutura analítica destinada à compreensão da sobrevivência estratégica dos Estados na Era Informacional, por meio da formulação da Teoria da Profundidade Estratégica Cibernética (TPEC)

A escolha de uma abordagem qualitativa fundamenta-se na natureza do problema investigado. Como o conceito de profundidade estratégica cibernética ainda não se encontra consolidado na literatura científica, torna-se necessária uma investigação voltada à construção conceitual e ao desenvolvimento teórico.

Ao mesmo tempo, a pesquisa possui caráter explicativo porque busca identificar mecanismos causais responsáveis pela relação entre a dependência digital, vulnerabilidade estratégica, soberania cibernética e resiliência estatal.

Nesse sentido, ela se situa na intersecção entre Geopolítica, Estudos Estratégicos, Relações Internacionais, Cibernética e Governança Digital.

4.2. A Estratégia Epistemológica

Do ponto de vista epistemológico, o estudo adota uma perspectiva realista-crítica. Parte-se do pressuposto de que as estruturas tecnológicas, econômicas e políticas que compõem o espaço cibernético produzem efeitos objetivos sobre a capacidade dos Estados de exercer soberania e preservar sua autonomia.

Entretanto, reconhece-se que tais estruturas são mediadas por fatores institucionais, culturais e cognitivos que influenciam a forma como os riscos e as ameaças são percebidos e enfrentados.

Essa abordagem permite integrar elementos materiais e imateriais na análise da profundidade estratégica contemporânea. Dessa forma, a pesquisa evita tanto o determinismo tecnológico quanto interpretações excessivamente construtivistas do poder cibernético.

4.3. O Método Hipotético-dedutivo

A investigação emprega o método hipotético-dedutivo como estratégia principal de construção teórica. Segundo essa abordagem, o conhecimento científico é produzido a partir da formulação de hipóteses passíveis de verificação empírica.

Assim, a pesquisa inicia-se com a identificação de uma lacuna teórica observada na literatura especializada.

Embora existam teorias consolidadas sobre: profundidade estratégica territorial, soberania cibernética, poder cibernético, resiliência nacional e soberania digital, não existe um modelo explicativo destinado a compreender como os Estados constroem profundidade estratégica em ambientes cibernéticos.

A partir dessa lacuna foi formulada a seguinte hipótese central: a sobrevivência estratégica dos Estados na Era Informacional depende mais da profundidade existente nas camadas física, lógica e cognitiva de seus ecossistemas cibernéticos do que da profundidade territorial clássica.

Essa hipótese orienta toda a construção da teoria proposta.

4.4. A Construção do Modelo Analítico

A elaboração do modelo foi realizada por meio da integração de conceitos provenientes de diferentes tradições teóricas.

Da Geopolítica Clássica foi incorporada a lógica da profundidade estratégica. Da teoria da Soberania Cibernética foram incorporadas as camadas física, lógica e cognitiva do espaço cibernético. Da literatura sobre Resiliência Nacional foi incorporada a noção de capacidade de absorção e recuperação diante de choques. Da teoria da Amazônia Cibernética foi incorporada a noção de patrimônio estratégico informacional.

A combinação desses elementos resultou na formulação de uma nova categoria analítica: a Profundidade Estratégica Cibernética.

4.5. A Operacionalização das Variáveis

Para permitir futura validação empírica da teoria, os conceitos foram convertidos em variáveis observáveis.

4.5.1. A Variável Dependente

- Profundidade Estratégica Cibernética (PEC): Corresponde ao grau de capacidade estrutural de um Estado para preservar a continuidade do exercício do Poder Nacional, da soberania cibernética e da autonomia decisória diante de ameaças, perturbações ou choques dirigidos às suas camadas física, lógica e cognitiva.

Ela não se limita à capacidade de resposta a incidentes específicos, representa uma propriedade sistêmica resultante da existência de mecanismos de redundância, diversificação, autonomia tecnológica, defesa cognitiva e resiliência institucional que ampliam a distância funcional entre uma ameaça e sua capacidade de produzir danos estratégicos irreversíveis.

Sob essa perspectiva, a Profundidade Estratégica Cibernética expressa o nível de proteção estrutural existente entre os ativos informacionais estratégicos de um Estado e os agentes capazes de comprometer sua estabilidade política, econômica, militar, psicossocial ou científico-tecnológica.

Quanto maior a Profundidade Estratégica Cibernética, maior será a capacidade estatal de absorver impactos sem perda significativa de funcionalidade; resistir a ataques dirigidos às infraestruturas críticas; adaptar-se a mudanças no ambiente tecnológico e geopolítico;

recuperar capacidades estratégicas após incidentes; e preservar a soberania cibernética e a autonomia nacional.

Assim, representa a capacidade estrutural de um Estado de manter sua soberania, autonomia decisória e continuidade funcional mediante a construção de camadas sucessivas de proteção, redundância, autonomia tecnológica e resiliência nas dimensões física, lógica e cognitiva do ciberespaço.

4.5.2. As Variáveis Independentes

- Capacidade Física (CF): Representa a robustez da infraestrutura material que sustenta o espaço cibernético, sendo vinculada à sua camada física. Materializa-se pelos seguintes indicadores: Data centers nacionais; Infraestruturas críticas protegidas; Cabos submarinos; Satélites; e Produção energética.

Tabela 1. Capacidade Física

Indicador	Métrica
Data centers nacionais	Número e capacidade instalada
Infraestruturas críticas protegidas	Percentual protegido
Energia	Índice de confiabilidade energética
Cabos submarinos	Quantidade e redundância
Satélites nacionais	Quantidade e capacidade operacional

Formula-se a seguinte hipótese: Quanto maior a Capacidade Física, maior a Profundidade Estratégica Cibernética.

- Capacidade Lógica (CL): Estabelece a autonomia tecnológica relacionada ao processamento da informação, sendo relacionada à camada lógica. Consolida-se pelos seguintes indicadores: Produção nacional de software; Inteligência artificial; Criptografia; Sistemas operacionais; e Plataformas digitais.

Tabela 2. Capacidade Lógica

Indicador	Métrica
Produção nacional de software	Participação no mercado
Inteligência Artificial	Produção científica e tecnológica
Criptografia soberana	Existência de soluções nacionais
Semicondutores	Capacidade produtiva
Computação avançada	Capacidade instalada

Formula-se a seguinte hipótese: Quanto maior a Capacidade Lógica, maior a Profundidade Estratégica Cibernética.

- Capacidade Cognitiva (CC): Consolida a capacidade social de resistir às operações de influência e manipulação, sendo direcionada à camada cognitiva. Materializa-se pelos seguintes indicadores: Alfabetização digital; Educação tecnológica; Confiança institucional; e Resiliência à desinformação.

Tabela 3. Capacidade Cognitiva

Indicador	Métrica
Alfabetização digital	Índice nacional

Educação STEM	Percentual da população
Confiança institucional	Pesquisas nacionais
Resiliência à desinformação	Índices internacionais
Defesa cognitiva	Existência de políticas públicas

Formula-se a seguinte hipótese: Quanto maior a Capacidade Cognitiva, maior a Profundidade Estratégica Cibernética.

- Dependência Tecnológica Externa (DT): Representa o grau de vulnerabilidade decorrente da dependência de tecnologias estrangeiras, sendo observada pelos seguintes indicadores: Dependência de nuvem estrangeira; Dependência de semicondutores; Dependência de plataformas digitais; e Dependência de modelos de inteligência artificial externos.

Tabela 4. Dependência Tecnológica Externa

Indicador	**Métrica**
Dependência de nuvem	Participação de provedores externos
Dependência de IA	Uso de modelos estrangeiros
Dependência de semicondutores	Importações estratégicas
Dependência de plataformas digitais	Participação de mercado
Dependência de sistemas operacionais	Uso em infraestruturas críticas

Formula-se a seguinte hipótese: Quanto maior a Dependência Tecnológica Externa, menor a Profundidade Estratégica Cibernética.

4.6. O Método de Validação

Para examinar a plausibilidade empírica da teoria proposta, emprega-se o método *Process Tracing*. Essa abordagem é amplamente utilizada em Estudos Estratégicos e Relações Internacionais para identificar mecanismos causais responsáveis pela ocorrência de determinado fenômeno.

O mecanismo causal investigado nesta pesquisa pode ser representado das seguintes formas:

A dependência tecnológica elevada gera vulnerabilidade estratégica, que indica uma maior exposição a ameaças sistêmicas. Esse contexto promove a redução da Profundidade Estratégica Cibernética, gerando menor capacidade de resiliência, o que causa a redução da soberania cibernética.

Em sentido inverso, o aumento da autonomia tecnológica promove o desenvolvimento da profundidade física, lógica e cognitiva. Esse conjunto gera maior resiliência estratégica, contribuindo para o fortalecimento da soberania cibernética e a sobrevivência estratégica do Estado.

Assim, a utilização do *Process Tracing* permite analisar não apenas resultados observáveis, mas também os processos que conduzem a esses resultados.

4.7. Seleção do Estudo de Caso

Como estratégia de validação preliminar, foi selecionado o ecossistema PIX brasileiro, fundamentando-se em quatro critérios:

- Relevância estratégica: O PIX tornou-se uma das principais infraestruturas digitais do Brasil;

- Dependência sistêmica: Sua operação afeta diretamente milhões de cidadãos, empresas e instituições financeiras;

- Disponibilidade de dados: O sistema possui ampla documentação pública e indicadores estatísticos acessíveis; e

- Existência de eventos críticos: O ecossistema já foi submetido a incidentes de segurança, campanhas de desinformação e desafios operacionais que permitem observar os mecanismos previstos pela teoria.

A análise do PIX possibilita avaliar simultaneamente as dimensões física, lógica e cognitiva da profundidade estratégica cibernética.

4.8. As Limitações da Pesquisa

Como toda investigação teórica, o presente estudo apresenta limitações. Em primeiro lugar, é uma formulação conceitual inicial que carece de uma maior validez empírica. Em segundo lugar, a operacionalização proposta para o Índice de Profundidade Estratégica Cibernética (IPEC) deverá ser refinada em pesquisas futuras por meio da incorporação de indicadores quantitativos e séries históricas.

Por fim, a presente investigação concentra-se prioritariamente na dimensão estatal, não explorando de forma aprofundada o papel desempenhado por corporações tecnológicas transnacionais.

Essas limitações, contudo, não comprometem a contribuição teórica do estudo, mas indicam oportunidades para futuras agendas de pesquisa.

5. A TEORIA DA PROFUNDIDADE ESTRATÉGICA CIBERNÉTICA

5.1. A Fundamentação Conceitual

A TPEC parte da premissa de que a transformação digital produziu uma mudança estrutural na natureza da competição internacional e, por conseguinte, nos mecanismos de preservação da soberania estatal.

Por séculos, a profundidade estratégica era entendida como uma propriedade relacionada ao espaço físico. A sobrevivência dos Estados dependia da capacidade de utilizar a geografia como instrumento de proteção, absorvendo ameaças por meio da distância territorial, da existência de barreiras naturais e da dispersão dos centros de poder.

A Era Informacional alterou significativamente essa lógica.

A crescente dependência das infraestruturas digitais reduziu a importância relativa da distância geográfica e ampliou a relevância dos ecossistemas informacionais como espaços centrais da competição estratégica.

Nesse contexto, a sobrevivência estratégica deixou de depender exclusivamente da profundidade territorial e passou a exigir a construção de profundidade em ambientes informacionais.

A TPEC surge precisamente para explicar esse fenômeno. A teoria sustenta que a capacidade de sobrevivência estratégica dos Estados no século XXI depende da construção de profundidade nas camadas física, lógica e cognitiva do espaço cibernético.

5.2. A Definição de Profundidade Estratégica Cibernética (PEC)

Define-se Profundidade Estratégica Cibernética como: O conjunto de capacidades estruturais que permite a um Estado absorver, resistir, adaptar-se e recuperar-se de perturbações dirigidas ao seu ecossistema cibernética sem perda significativa de autonomia política, funcionalidade institucional ou capacidade de projeção de poder.

Diferentemente da profundidade estratégica clássica, medida pela extensão territorial, a profundidade estratégica cibernético é calculada pela capacidade funcional de resistência de um ecossistema cibernético.

Em outras palavras, trata-se da distância estratégica existente entre uma ameaça informacional e a capacidade dessa ameaça de produzir danos irreversíveis aos interesses nacionais.

Em síntese, quanto maior essa distância funcional, maior será a profundidade estratégica cibernética.

5.3. Os Fundamentos da Teoria

A TPEC está fundamentada em quatro pressupostos centrais:

- Primeiro (A informação tornou-se recurso estratégico): A Era Industrial foi marcada pela centralidade dos recursos materiais.

A Era Informacional caracteriza-se pela centralidade dos recursos informacionais. Os dados, algoritmos, inteligência artificial, capacidade computacional e conhecimento tecnológico passaram a exercer papel equivalente ao desempenhado por recursos naturais estratégicos em períodos anteriores. Consequentemente, a proteção desses elementos tornou-se questão de segurança nacional.

- Segundo (A soberania tornou-se multidimensional): A soberania contemporânea não pode mais ser compreendida apenas em termos absolutos. É fundamental, então, dividir o conceito geral de soberania em várias dimensões que estão ligadas ao território em que são aplicadas. Portanto, é necessário admitir que existem frações de soberania que exercem efeitos nos âmbitos terrestre, marítimo, aéreo, sideral e cibernético. Assim, a capacidade estatal de exercer autoridade depende crescentemente do controle relativo sobre infraestruturas digitais, fluxos informacionais e ambientes cognitivos. Ela passa a envolver simultaneamente dimensões físicas, lógicas e cognitivas.

- Terceiro (A vulnerabilidade estratégica é determinada pela dependência tecnológica): Na Era Informacional, a vulnerabilidade de um Estado não decorre apenas de ameaças externas. Ela decorre também do grau de dependência tecnológica existente.

Quanto maior a dependência de infraestruturas, plataformas, semicondutores, sistemas operacionais ou modelos de inteligência artificial controlados por atores externos, menor será a autonomia estratégica nacional.

- Quarto (A resiliência é produto da profundidade estratégica): A resiliência não constitui fenômeno espontâneo. Ela resulta da existência prévia de mecanismos de redundância, autonomia, diversificação e proteção. Desta forma, a profundidade estratégica cibernética representa precisamente o conjunto dessas capacidades.

5.4. As Três Camadas da Profundidade Estratégica Cibernética (PEC)

A teoria propõe que a profundidade estratégica cibernética é construída sobre três camadas interdependentes.

A camada física constitui o nível estrutural da profundidade estratégica. Ela corresponde à infraestrutura material responsável pelo funcionamento do espaço cibernético, incluindo: centros de dados; redes de telecomunicações; cabos submarinos; satélites; sistemas energéticos; semicondutores; e minerais estratégicos. Consequentemente, a profundidade física depende da capacidade de proteger, diversificar e redundar essas infraestruturas.

Um Estado que concentra seus sistemas críticos em poucos pontos vulneráveis possui baixa profundidade física. Por outro lado, um Estado que dispõe de redundância energética, múltiplas rotas de comunicação e infraestrutura distribuída apresenta maior capacidade de absorção de choques.

A camada lógica corresponde aos sistemas responsáveis pelo processamento, armazenamento e circulação da informação, incluindo: softwares; sistemas operacionais; protocolos; algoritmos; plataformas digitais; e sistemas de inteligência artificial.

A profundidade lógica depende da autonomia tecnológica. Quanto maior a capacidade nacional de desenvolver e controlar tecnologias críticas, maior a sua profundidade estratégica. A dependência excessiva de tecnologias estrangeiras cria vulnerabilidades estruturais capazes de comprometer a autonomia decisória dos Estados.

A camada cognitiva constitui a dimensão mais complexa e estratégica da teoria, compreendendo: indivíduos; percepções; crenças; valores; identidades; e processos decisórios.

Historicamente, os conflitos buscavam destruir recursos físicos. Contudo, na Era Informacional, torna-se possível influenciar diretamente a percepção dos indivíduos e das instituições. As operações de influência, campanhas de desinformação, manipulação algorítmica e guerra cognitiva passaram a integrar o repertório das disputas estratégicas contemporâneas.

Assim, a profundidade cognitiva corresponde à capacidade de uma sociedade em resistir a esses processos de manipulação. Uma sociedade capaz de identificar desinformação, preservar a confiança institucional e manter a coesão social apresenta elevada profundidade cognitiva.

5.5. O Mecanismo de Produção da Profundidade Estratégica Cibernética (PEC)

A Teoria da Profundidade Estratégica Cibernética sustenta que a PEC não constitui um atributo natural dos Estados, mas o resultado de um processo contínuo de construção institucional, tecnológica e social.

Assim como a profundidade estratégica territorial foi historicamente produzida por fatores geográficos, infraestrutura militar e capacidade logística, a profundidade estratégica cibernética emerge da combinação de mecanismos capazes de ampliar a distância funcional entre uma ameaça e sua capacidade de produzir danos estratégicos irreversíveis.

A teoria identifica quatro mecanismos estruturantes responsáveis pela produção da Profundidade Estratégica Cibernética: redundância, diversificação, autonomia e resiliência. Esses mecanismos atuam simultaneamente sobre as camadas física, lógica e cognitiva do ciberespaço, formando sucessivas barreiras de proteção capazes de reduzir vulnerabilidades sistêmicas e preservar a continuidade do Poder Nacional.

5.5.1. A Redundância

A redundância constitui o primeiro mecanismo de produção da PEC. Ela corresponde à existência de recursos, sistemas ou capacidades alternativas capazes de assumir funções críticas quando os componentes principais são comprometidos.

Na dimensão física, a redundância manifesta-se por meio da existência de múltiplos data centers, rotas alternativas de telecomunicações, sistemas energéticos de contingência e infraestrutura distribuída. Na dimensão lógica, expressa-se pela disponibilidade de softwares alternativos, ambientes computacionais de reserva e sistemas de recuperação de dados. Na dimensão cognitiva, ocorre por meio da pluralidade de canais informacionais e da existência de instituições capazes de preservar a confiança pública durante períodos de crise.

A função estratégica da redundância consiste em impedir que um único ponto de falha seja capaz de comprometer o funcionamento do sistema como um todo. Quanto maior a redundância existente, maior será a capacidade do Estado de manter a continuidade operacional diante de ataques, falhas técnicas ou desastres.

5.5.2. A Diversificação

A diversificação corresponde ao mecanismo destinado a reduzir a concentração de riscos estratégicos. Diferentemente da redundância, que busca criar sistemas alternativos para a mesma função, a diversificação procura evitar a dependência excessiva de um único fornecedor, tecnologia, infraestrutura ou fonte de recursos.

No plano físico, a diversificação envolve a multiplicidade de fornecedores de equipamentos, fontes energéticas e rotas de conectividade internacional. Na camada lógica, envolve a utilização de diferentes arquiteturas tecnológicas, plataformas digitais e ecossistemas de software. Na dimensão cognitiva, manifesta-se por meio da pluralidade de fontes de informação e da diversidade institucional responsável pela formação da opinião pública.

A diversificação reduz a vulnerabilidade a interrupções decorrentes de sanções econômicas, embargos tecnológicos, falhas sistêmicas ou ações coercitivas de atores externos. Consequentemente, amplia a liberdade de ação do Estado e fortalece sua autonomia estratégica.

5.5.3. A Autonomia

A autonomia constitui o mecanismo central da Profundidade Estratégica Cibernética. Ela corresponde à capacidade de um Estado

desenvolver, operar, manter e evoluir tecnologias críticas sem depender integralmente de atores externos.

A autonomia física está relacionada ao controle de infraestruturas críticas, recursos energéticos e sistemas de comunicação. A autonomia lógica refere-se à capacidade nacional de produzir software, inteligência artificial, sistemas criptográficos, semicondutores e plataformas digitais estratégicas. A autonomia cognitiva diz respeito à capacidade que tem a sociedade de produzir as suas próprias agendas políticas, económicas e culturais sem sofrer demasiada influência de atores externos.

A autonomia não pressupõe autossuficiência absoluta, condição praticamente impossível em sistemas tecnológicos globais altamente interdependentes. Seu objetivo consiste em garantir que eventuais interrupções externas não comprometam a continuidade das funções essenciais do Estado.

Sob a perspectiva da TPEC, a dependência tecnológica excessiva representa o principal fator redutor da profundidade estratégica, enquanto a autonomia tecnológica constitui seu fator de expansão mais importante.

5.5.4. A Resiliência

A resiliência representa o resultado operacional da interação entre redundância, diversificação e autonomia. Ela corresponde à capacidade de absorver impactos, adaptar-se a condições adversas e recuperar funcionalidades essenciais sem perda significativa da soberania ou da capacidade decisória.

Na camada física, a resiliência manifesta-se pela célere restauração de infraestruturas críticas após incidentes. Na camada lógica, expressa-se pela recuperação de sistemas comprometidos e pela continuidade do processamento informacional. Na camada cognitiva, traduz-se na capacidade da sociedade de preservar a confiança institucional e resistir a operações de influência e desinformação.

A resiliência não elimina vulnerabilidades, mas reduz sua capacidade de produzir efeitos estratégicos duradouros. Dessa forma, constitui a expressão prática da profundidade estratégica construída pelos demais mecanismos.

5.5.5. O Processo de Formação da Profundidade Estratégica Cibernética

A teoria propõe que a Profundidade Estratégica Cibernética emerge da interação cumulativa desses quatro mecanismos. A redundância reduz a probabilidade de colapso; a diversificação reduz a concentração de riscos; a autonomia reduz a dependência externa; e a resiliência garante a capacidade de recuperação.

O efeito combinado desses mecanismos produz sucessivas camadas de proteção que ampliam a distância funcional entre uma ameaça e sua capacidade de comprometer a continuidade do Poder Nacional. Quanto mais desenvolvidos forem esses mecanismos, maior será a profundidade estratégica cibernética do Estado.

A PEC constitui o resultado acumulado de capacidades estruturais que permitem ao Estado resistir, adaptar-se e sobreviver em um ambiente caracterizado por crescente competição tecnológica, dependência digital e vulnerabilidade informacional.

5.6. A Lei da Profundidade Estratégica Cibernética

A Teoria da Profundidade Estratégica Cibernética culmina na formulação de sua proposição causal central, denominada Lei da Profundidade Estratégica Cibernética (LPEC). Essa lei sintetiza o mecanismo explicativo da teoria ao estabelecer a relação entre capacidades estruturais do Estado, autonomia tecnológica, resiliência informacional e sobrevivência estratégica na Era Informacional.

Diferentemente da profundidade estratégica clássica, cuja efetividade estava associada predominantemente à extensão territorial e à existência de barreiras geográficas, a profundidade estratégica cibernética é determinada pela capacidade de um Estado construir camadas sucessivas de proteção, redundância, autonomia e resiliência em seu ecossistema informacional.

A LPEC pode ser expressa da seguinte forma:

A capacidade de sobrevivência estratégica de um Estado na Era Informacional é diretamente proporcional ao grau de profundidade existente nas camadas física, lógica e cognitiva do seu ecossistema cibernético e inversamente proporcional ao seu nível de dependência tecnológica externa.

Essa formulação estabelece uma relação causal entre capacidades nacionais e sobrevivência estratégica. A teoria sustenta que a autonomia de um Estado não decorre exclusivamente da posse de recursos materiais ou da extensão do território, mas da capacidade de proteger, controlar e sustentar os sistemas responsáveis pela produção, processamento, circulação e utilização da informação.

A lei da Profundidade Estratégica Cibernética parte do pressuposto de que o ciberespaço se tornou uma dimensão essencial da soberania contemporânea. Nesse ambiente, a vulnerabilidade estratégica não é determinada apenas pela exposição física a ameaças externas, mas também pela dependência tecnológica, pela fragilidade institucional e pela suscetibilidade da sociedade a processos de manipulação informacional.

Consequentemente, a sobrevivência estratégica deixa de ser explicada apenas pela capacidade de defesa territorial e passa a depender da robustez estrutural do ecossistema informacional nacional.

5.6.1. A Estrutura Causal da Lei

A LPEC propõe que a sobrevivência estratégica resulte de um processo cumulativo de fortalecimento das capacidades nacionais.

O primeiro estágio corresponde à construção das capacidades física, lógica e cognitiva. Essas capacidades formam a base estrutural da soberania cibernética.

O segundo estágio corresponde à produção da profundidade estratégica por meio dos mecanismos de redundância, diversificação, autonomia e resiliência.

O terceiro estágio corresponde à ampliação da capacidade de absorver, resistir, adaptar-se e recuperar-se de ameaças sistêmicas.

O resultado final desse processo é a preservação da soberania cibernética, da autonomia decisória e da continuidade do Poder Nacional.

A dependência tecnológica externa atua como variável redutora da profundidade estratégica. Quanto maior a dependência de plataformas digitais, semicondutores, sistemas operacionais, serviços de computação em nuvem ou modelos de inteligência artificial controlados por atores externos, menor será a autonomia estratégica do Estado. Além disso, maior será sua vulnerabilidade a mecanismos de coerção tecnológica, sanções econômicas ou interrupções sistêmicas.

5.6.2. O Princípio da Distância Funcional

A principal inovação da LPEC consiste na substituição do conceito clássico de distância geográfica pelo de distância funcional.

Na geopolítica tradicional, a profundidade estratégica era medida pela distância física existente entre as fronteiras e os centros vitais de poder. Na Era Informacional, entretanto, uma ameaça pode atravessar continentes em segundos e atingir diretamente infraestruturas críticas sem qualquer deslocamento territorial.

Dessa forma, a profundidade estratégica passa a ser definida pela distância funcional existente entre uma ameaça e sua capacidade de produzir danos irreversíveis ao sistema nacional.

Quanto maior o número de barreiras institucionais, tecnológicas, cognitivas e operacionais que uma ameaça precisa superar para comprometer os interesses estratégicos nacionais, maior será a profundidade estratégica cibernética do Estado.

5.6.3. Os Corolários da Lei

Da LPEC derivam-se cinco corolários fundamentais:

Corolário 1: Os Estados com elevada autonomia tecnológica tendem a apresentar maior profundidade estratégica cibernética;

Corolário 2: Os Estados capazes de controlar simultaneamente as camadas física, lógica e cognitiva do ciberespaço apresentam maior capacidade de sobrevivência estratégica;

Corolário 3: A dependência tecnológica externa reduz a profundidade estratégica, mesmo em países com elevada infraestrutura física;

Corolário 4: A resiliência estratégica é consequência da profundidade estratégica previamente construída e não sua causa primária; e

Corolário 5: Na Era Informacional, a distribuição internacional de poder tende a favorecer os Estados que possuem maior profundidade estratégica cibernética.

5.6.4. O Alcance Teórico da Lei

A LPEC não pretende substituir as teorias clássicas da geopolítica ou da estratégia. Sua contribuição consiste em ampliar essas abordagens para um contexto caracterizado pela centralidade da informação, da conectividade e da competição tecnológica.

Assim como a profundidade territorial foi um dos fundamentos da sobrevivência dos Estados na Era Industrial. Os resultados sugerem que a profundidade estratégica cibernética pode constituir um fator relevante para a preservação da soberania estatal na Era Informacional.

Sob essa perspectiva, a LPEC constitui o princípio explicativo central da TPEC, permitindo compreender por que alguns Estados conseguem preservar sua autonomia diante de choques tecnológicos e informacionais, enquanto outros permanecem estruturalmente vulneráveis à dependência digital e à coerção cibernética.

5.7. A Profundidade Estratégica Cibernética Como Nova Projeção do Poder Nacional

A principal contribuição da TPEC consiste em ampliar a teoria clássica da profundidade estratégica para o contexto da Era Informacional.

A profundidade estratégica deixa de ser interpretada exclusivamente como atributo geográfico e passa a ser compreendida como capacidade sistêmica de resistência.

A teoria propõe que a PEC constitui uma nova projeção do Poder Nacional, capaz de influenciar simultaneamente: a soberania; a segurança nacional; a competitividade econômica; a estabilidade institucional; a capacidade de inovação; e a projeção internacional do Estado.

Sob essa perspectiva, os Estados que conseguirem construir profundidade física, lógica e cognitiva estarão mais aptos a preservar sua autonomia em um ambiente caracterizado por crescente competição tecnológica e informacional.

A TPEC oferece, assim, uma estrutura conceitual destinada a compreender a sobrevivência estratégica na Era Informacional, da

mesma forma que a Geopolítica clássica buscou compreender a sobrevivência estatal na Era Industrial.

Essa formulação constitui o núcleo teórico da presente pesquisa e fundamenta as análises empíricas desenvolvidas nas seções subsequentes.

6. O ÍNDICE DE PROFUNDIDADE ESTRATÉGICA CIBERNÉTICA (IPEC).

6.1. A Fundamentação do Índice

Uma das principais limitações das teorias estratégicas contemporâneas reside na dificuldade de transformar conceitos abstratos em variáveis observáveis e comparáveis. Embora conceitos como poder nacional, soberania digital, resiliência nacional e autonomia tecnológica sejam amplamente utilizados na literatura especializada, sua mensuração permanece frequentemente dependente de avaliações qualitativas.

A Teoria da Profundidade Estratégica Cibernética propõe superar essa limitação por meio da criação do Índice de Profundidade Estratégica Cibernética (IPEC).

O objetivo do IPEC é fornecer um instrumento analítico capaz de medir, comparar e monitorar a capacidade dos Estados em construir profundidade estratégica nos seus ecossistemas cibernéticos.

Ele permite avaliar o grau de preparação dos Estados para enfrentar ameaças dirigidas às infraestruturas digitais, aos sistemas tecnológicos e aos ambientes cognitivos. Além disso, possibilita

identificar vulnerabilidades estruturais que podem comprometer a soberania e a autonomia nacional.

A construção do índice baseia-se diretamente nos fundamentos da Teoria da Profundidade Estratégica Cibernética, especialmente na interação entre as dimensões física, lógica e cognitiva do espaço cibernético.

6.2. A Estrutura Conceitual do IPEC

O IPEC é composto por quatro grandes dimensões.

- dimensão Física (F): Avalia a robustez da infraestrutura material responsável pelo funcionamento do ecossistema informacional nacional;

- dimensão Lógica (L): Avalia a autonomia tecnológica e a capacidade de desenvolvimento de sistemas digitais estratégicos;

- dimensão Cognitiva (C): Avalia a capacidade da sociedade de resistir à manipulação informacional e preservar sua autonomia decisória; e

- dependência Tecnológica Externa (DT): Mede o nível de suscetibilidade que advém da dependência de tecnologias controladas por agentes externos.

Enquanto as três primeiras dimensões contribuem positivamente para a profundidade estratégica, a dependência tecnológica exerce influência negativa sobre o índice.

A dimensão física representa a base estrutural da profundidade estratégica cibernética. Ela corresponde à infraestrutura material responsável pela sustentação dos fluxos digitais nacionais.

A avaliação dessa dimensão será realizada a partir dos seguintes indicadores:

a. infraestrutura de Telecomunicações

Cobertura nacional de redes de comunicação;

- capacidade de tráfego de dados; e
- diversidade de rotas de conectividade.

b. centros de Dados

- quantidade de data centers estratégicos;
- capacidade nacional de armazenamento; e
- distribuição geográfica da infraestrutura.
- infraestrutura Energética
- confiabilidade do sistema elétrico;
- capacidade de redundância; e
- resiliência energética.

d. infraestrutura Espacial

- satélites próprios; e
- sistemas nacionais de posicionamento e observação.

e. cabos Submarinos

- número de conexões internacionais; e
- diversificação das rotas de comunicação.

A dimensão lógica mede a capacidade nacional de controlar os mecanismos tecnológicos responsáveis pelo processamento e circulação da informação.

Os indicadores propostos incluem:

a. produção Nacional de Software

- participação da indústria nacional; e
- capacidade de desenvolvimento de sistemas críticos.

b. Inteligência Artificial

- investimentos em IA;
- produção científica; e
- ecossistemas nacionais de inovação.
- c. Criptografia
- desenvolvimento de soluções criptográficas próprias.

- d. Computação Avançada
- supercomputação;
- computação quântica; e
- infraestrutura de processamento de alto desempenho.
- e. Plataformas Digitais
- existência de plataformas nacionais relevantes; e
- capacidade de reduzir dependências externas.

A dimensão cognitiva representa a principal inovação da Teoria da Profundidade Estratégica Cibernética. Historicamente, os indicadores de poder concentraram-se em recursos materiais.

A TPEC parte do entendimento de que a capacidade de uma sociedade resistir à manipulação informacional tornou-se fator estratégico.

Os indicadores propostos incluem:

a. Alfabetização Digital

- capacidade da população de utilizar tecnologias digitais de forma crítica.

b. Educação Científica e Tecnológica

- formação em áreas STEM; e

- produção de capital humano qualificado.

c. Confiança Institucional

- níveis de confiança nas instituições públicas.

d. Resiliência à Desinformação

- capacidade de identificar informações falsas; e
- existência de mecanismos de verificação.

e. Defesa Cognitiva

- estratégias nacionais voltadas à proteção do ambiente informacional.

Cabe ressaltar que a pontuação das dimensões varia de 0 a 100.

A dependência tecnológica constitui variável redutora do índice. A hipótese central da teoria sustenta que a autonomia estratégica diminui à medida que aumenta a dependência de tecnologias críticas controladas por atores externos.

Os indicadores incluem:

a. Dependência de Computação em Nuvem

- participação de provedores estrangeiros no armazenamento e processamento de dados nacionais.

b. Dependência de Semicondutores

- capacidade nacional de produzir componentes estratégicos.

c. Dependência de Plataformas Digitais

- concentração de serviços digitais em empresas estrangeiras.

d. Dependência de Inteligência Artificial

- utilização predominante de modelos de IA desenvolvidos fora do país.

e. Dependência de Sistemas Operacionais

- grau de utilização de softwares estrangeiros em sistemas críticos.

A pontuação da dependência tecnológica varia de 0 a 100. Quanto maior essa pontuação, menor será a profundidade estratégica cibernética.

Para operacionalizar os conceitos centrais da TPEC, foi desenvolvida a sua matriz analítica, que permite sua utilização em estudos comparativos, avaliações estratégicas nacionais e futuras pesquisas quantitativas.

A matriz estabelece a relação entre os componentes estruturantes da teoria, os mecanismos causais observáveis, os indicadores empíricos e seus efeitos sobre a sobrevivência estratégica dos Estados.

Sua principal função consiste em transformar os conceitos abstratos da TPEC em categorias analíticas passíveis de observação,

mensuração e comparação.

Tabela 5. Matriz Analítica

Dimensão Estratégica	Objetivo Estratégico	Componentes Principais	Indicadores Empíricos	Vulnerabilidades Associadas	Impac sobre Profun ade Estraté a
Física	Garantir continuidade operacional	Infraestruturas críticas, energia, telecomun	Capacidade energética, redundânc	Ataques físicos, sabotagem, interrupçã	Alto

⚠ Esta tabela possui muitas colunas e foi cortada para impressão. Para visualizá-la completa, acesse o artigo original em: https://revistatopicos.com.br/artigos/a-teoria-da-profundidade-estrategica-cibernetica-soberania-resiliencia-e-poder-nacional-na-era-informacional?noblockage

6.3. A Formulação Matemática do IPEC

Como a TPEC afirma, as três camadas do espaço cibernético são interdependentes e que uma deficiência grave em qualquer uma delas reduz a profundidade estratégica do sistema.

IPEC = (0,30CF + 0,30CL + 0,30CC) - (0,10DT)

Onde:

- IPEC = Índice de Profundidade Estratégica Cibernética;
- CF = Capacidade Física;

- CL = Capacidade Lógica;
- CC = Capacidade Cognitiva; e
- DT = Dependência Tecnológica Externa.

Sendo:

- CF, CL e CC normalizados entre 0 e 1;
- DT normalizado entre 0 e 1;

A formulação matemática do Índice de Profundidade Estratégica Cibernética (IPEC) foi concebida para refletir os pressupostos centrais da Teoria da Profundidade Estratégica Cibernética (TPEC). O modelo parte da premissa de que a profundidade estratégica de um Estado resulta da interação equilibrada entre três dimensões estruturantes do ciberespaço: a capacidade física, a capacidade lógica e a capacidade cognitiva.

Por essa razão, atribuiu-se peso equivalente de 30% para cada uma dessas dimensões. A distribuição simétrica dos pesos decorre do entendimento de que nenhuma delas é suficiente, isoladamente, para assegurar a soberania cibernética ou a sobrevivência estratégica do Estado. A fragilidade em qualquer uma das camadas pode comprometer a resiliência do sistema como um todo, em conformidade com o princípio da vulnerabilidade do elo mais fraco observado em sistemas complexos.

A variável Dependência Tecnológica Externa (DT) recebeu peso negativo de 10%, uma vez que não constitui uma dimensão geradora de profundidade estratégica, mas sim um fator redutor da

autonomia nacional. Sua inclusão visa capturar o impacto das vulnerabilidades decorrentes da dependência de tecnologias, plataformas, semicondutores, serviços de computação em nuvem e modelos de inteligência artificial controlados por atores externos.

Dessa forma, a estrutura matemática do índice permite que os ganhos produzidos pelas capacidades física, lógica e cognitiva sejam parcialmente reduzidos pelos efeitos da dependência tecnológica externa, refletindo a hipótese central da teoria de que a autonomia tecnológica amplia a profundidade estratégica, enquanto a dependência tecnológica a reduz.

A configuração adotada gera uma faixa teórica de variação entre -10 e 90 pontos. O valor máximo é alcançado quando as três capacidades atingem sua pontuação máxima e a dependência tecnológica externa é inexistente. O valor mínimo ocorre quando as capacidades estruturantes são nulas e a dependência tecnológica externa atinge seu nível máximo. Essa característica não representa uma limitação do índice, mas uma escolha metodológica deliberada destinada a evidenciar que a dependência tecnológica exerce efeito corrosivo sobre a profundidade estratégica cibernética.

Para fins comparativos internacionais e futuras aplicações quantitativas, recomenda-se que o IPEC seja interpretado segundo faixas de classificação previamente definidas ou, alternativamente, convertido para uma escala normalizada de 0 a 100 pontos, sem prejuízo de sua lógica teórica original.

Essa postura é fundamentada em três argumentos centrais:

a. A equivalência estrutural: A camada física fornece a infraestrutura material necessária ao funcionamento do ecossistema cibernético; a

camada lógica fornece os mecanismos tecnológicos responsáveis pelo processamento e circulação da informação; e a camada cognitiva fornece a legitimidade social, a confiança institucional e a capacidade de resistência às operações de influência.

Nenhuma dessas dimensões é suficiente isoladamente para garantir soberania cibernética.

Um Estado pode possuir infraestrutura avançada, mas permanecer vulnerável caso dependa tecnologicamente de atores externos. Da mesma forma, pode possuir elevada autonomia tecnológica, mas apresentar fragilidade diante de campanhas de desinformação capazes de comprometer sua estabilidade política.

A atribuição de pesos equivalentes reflete essa condição de interdependência estrutural.

b. O princípio da vulnerabilidade do “Elo Mais Fraco”: A literatura sobre resiliência de sistemas complexos demonstra que a robustez de uma estrutura depende de seu componente mais vulnerável. Na Era Informacional, um colapso em qualquer uma das três camadas pode produzir efeitos sistêmicos, como:

- Ataques a infraestruturas críticas comprometem a camada física;
- Dependência de software estrangeiro compromete a camada lógica;
- Operações de influência comprometem a camada cognitiva.

Consequentemente, não existe fundamento teórico suficiente para privilegiar uma dimensão em detrimento das demais na formulação inicial do índice.

c. A coerência com a Teoria da Soberania Cibernética: A divisão tripartite entre camadas física, lógica e cognitiva deriva diretamente da literatura sobre soberania cibernética e governança do ciberespaço. A TPEC amplia essa estrutura ao transformá-la em mecanismo explicativo da sobrevivência estratégica.

A manutenção de pesos equivalentes preserva a coerência entre o modelo teórico e sua operacionalização empírica.

A variável Dependência Tecnológica Externa (DT) recebe peso negativo, pois não representa uma dimensão constitutiva da profundidade estratégica, mas um fator redutor da autonomia nacional. Sua inclusão decorre da hipótese de que a dependência tecnológica funciona como uma vulnerabilidade transversal capaz de limitar os efeitos positivos das demais capacidades.

Um Estado pode apresentar elevada infraestrutura física, boa capacidade cognitiva, razoável desenvolvimento tecnológico, mas ainda assim permanecer vulnerável caso dependa fortemente de semicondutores estrangeiros, provedores externos de nuvem, sistemas operacionais estrangeiros, e plataformas digitais controladas por outros países.

A escolha do peso negativo para a dependência tecnológica permite que ela não anule completamente os ganhos produzidos pelas demais dimensões, mas garante que a mesma exerça influência significativa sobre o resultado.

Tabela 6. Peso e faixa de pontuação das camadas

Dimensão	Peso (%)	Faixa de Pontuação
Física	30	0–100
Lógica	30	0–100
Cognitiva	30	0–100
DT	-10	0–100

Foram utilizadas as seguintes fontes para a coleta de dados, sendo elas indexadas à base de dados vinculada ao índice:

- Dimensão Física

International Telecommunication Union (ITU);

World Bank Data;

GSMA Intelligence;

International Energy Agency (IEA); e

International Data Corporation (IDC).

- Dimensão Lógica

UNESCO Science Report;

WIPO Global Innovation Index;

Stanford AI Index; e

OECD Digital Economy Outlook.

- Imensão Cognitiva

OECD Education Database;

Reuters Digital News Report;

Edelman Trust Barometer; e

UN E-Government Survey.

- Dependência Tecnológica

Gartner;

Statista;

Semiconductor Industry Association;

World Semiconductor Trade Statistics.

Os pesos propostos devem ser compreendidos como uma formulação teórica inicial. Em futuras pesquisas, poderão ser refinados por meio de técnicas quantitativas como:

- Análise Fatorial Exploratória (AFE);
- Análise Fatorial Confirmatória (AFC);
- Principal Component Analysis (PCA);
- Analytic Hierarchy Process (AHP); e

- Modelagem de Equações Estruturais (SEM).

Esses procedimentos permitirão verificar empiricamente se as três dimensões possuem efetivamente contribuição equivalente para a profundidade estratégica cibernética ou se determinados contextos nacionais exigem ponderações diferenciadas.

Assim, os pesos adotados nesta versão da teoria possuem caráter heurístico e teoricamente fundamentado, servindo como ponto de partida para a validação empírica da Teoria da Profundidade Estratégica Cibernética.

6.4. A Clusterização do IPEC

O Índice de Profundidade Estratégica Cibernético varia de 0 a 100 pontos. A classificação proposta não representa apenas uma divisão estatística da escala, mas níveis crescentes de autonomia, resiliência e soberania cibernética

Tabela 7. Escala de Classificação Estratégica da Profundidade Estratégica Cibernética

Faixa	Classificação	Características Estratégicas	Papel no Ecossistema Cibernético
-10 a 14,9	Crítica	Estado altamente dependente de tecnologias externas, com baixa capacidade de proteção de infraestruturas críticas, reduzida autonomia tecnológica e elevada vulnerabilidade cognitiva.	Sobrevivência Assistida (Vulnerável)

15 a 29,9	Muito Baixa	Estado com graves limitações estruturais nas dimensões física, lógica e cognitiva, apresentando elevada exposição a riscos tecnológicos e informacionais.	Sobrevivência Dependente (Dependente)
30 a 44,9	Baixa	Estado com capacidades cibernéticas limitadas, baixa autonomia tecnológica e reduzida capacidade de absorção de choques sistêmicos.	Autonomia Restrita (Dependente Emergente)
45 a 59,9	Média	Estado em processo de consolidação de capacidades estratégicas, possuindo infraestrutura relevante, mas ainda dependente de atores externos em setores críticos.	Autonomia Parcial (Emergente)
60 a 74,9	Alta	Estado resiliente, com autonomia significativa em áreas estratégicas, elevada capacidade de recuperação diante de crises e reduzida dependência tecnológica.	Autonomia Estratégica (Resiliente)
75 a 90	Muito Alta	Potência cibernética consolidada, caracterizada por elevada autonomia tecnológica, forte capacidade inovadora, robustez institucional e baixa vulnerabilidade sistêmica.	Liderança Informacional (Potência Cibernética)

A definição das faixas do Índice de Profundidade Estratégica Cibernética (IPEC) decorre diretamente da Lei da Profundidade Estratégica Cibernética (LPEC), segundo a qual a capacidade de sobrevivência estratégica de um Estado na Era Informacional é

proporcional à profundidade existente nas camadas física, lógica e cognitiva do seu ecossistema cibernético e inversamente proporcional ao seu nível de dependência tecnológica externa.

A classificação proposta não representa apenas uma escala quantitativa, mas uma tipologia qualitativa dos níveis de autonomia, resiliência e soberania cibernética alcançados pelos Estados.

a. Faixa Crítica (-10 a 14,9): Os Estados classificados nesta faixa apresentam profundidade estratégica cibernética insuficiente para assegurar a continuidade de suas funções essenciais diante de choques tecnológicos, cibernéticos ou informacionais. Caracterizam-se por elevada dependência de tecnologias estrangeiras, baixa capacidade de proteção das infraestruturas críticas, reduzida autonomia tecnológica e limitada resiliência cognitiva. Nessas condições, a sobrevivência estratégica do Estado depende frequentemente do apoio externo, seja por meio de alianças internacionais, assistência tecnológica ou suporte de empresas transnacionais. A capacidade de resposta a incidentes é reduzida, tornando o país altamente suscetível à coerção tecnológica, interrupções de serviços essenciais e operações de influência;

b. Faixa Muito Baixa (15 a 29,9): Os Estados enquadrados nesta faixa possuem capacidades cibernéticas incipientes e enfrentam significativas limitações estruturais. Embora disponham de algumas infraestruturas digitais e mecanismos básicos de governança, permanecem altamente dependentes de tecnologias, plataformas e serviços controlados por atores externos. A profundidade estratégica existente é insuficiente

para garantir autonomia decisória plena. Em situações de crise sistêmica, a capacidade de absorção e recuperação tende a ser limitada, ampliando a vulnerabilidade nacional a ataques cibernéticos, interrupções tecnológicas e campanhas de desinformação;

c. Faixa Baixa (30 a 44,9): Nesta faixa encontram-se Estados que iniciaram o processo de fortalecimento de suas capacidades físicas, lógicas e cognitivas, mas ainda apresentam vulnerabilidades significativas em setores estratégicos. A infraestrutura digital é funcional, porém a autonomia tecnológica permanece limitada. Embora possuam condições de responder a incidentes de menor intensidade, a dependência de tecnologias externas continua representando um fator relevante de risco. Esses países apresentam capacidade restrita de projeção de poder no ciberespaço e enfrentam dificuldades para reduzir vulnerabilidades estruturais de longo prazo;

d. Faixa Média (45 a 59,9): Os Estados classificados nesta categoria apresentam profundidade estratégica cibernética em consolidação. Possuem infraestrutura relativamente robusta, instituições mais resilientes e níveis moderados de autonomia tecnológica. Entretanto, permanecem dependentes de atores externos em áreas críticas, como semicondutores, computação em nuvem, plataformas digitais ou inteligência artificial. A capacidade de absorver e recuperar-se de choques é significativa, permitindo a preservação das funções essenciais do Estado. Todavia, persistem vulnerabilidades capazes de comprometer a autonomia

estratégica em cenários de competição tecnológica prolongada;

e. Faixa Alta (60 a 74,9): Esta faixa representa Estados que alcançaram elevado grau de profundidade estratégica cibernética. Suas capacidades físicas, lógicas e cognitivas encontram-se amplamente desenvolvidas, proporcionando elevada resiliência diante de ameaças sistêmicas. Esses países possuem autonomia significativa em setores tecnológicos estratégicos, mecanismos avançados de proteção das infraestruturas críticas e elevada capacidade de defesa cognitiva. Embora ainda mantenham algum grau de interdependência tecnológica internacional, essa dependência não compromete sua liberdade de ação nem sua capacidade de resposta a crises; e

f. faixa Muito Alta (75 a 90): Os Estados classificados nesta faixa constituem as principais potências cibernéticas do sistema internacional. Possuem elevada autonomia tecnológica, domínio de tecnologias críticas, forte capacidade de inovação, infraestrutura altamente resiliente e mecanismos avançados de defesa cognitiva. Sua profundidade estratégica cibernética permite absorver, resistir e recuperar-se de ameaças complexas sem comprometer significativamente a soberania nacional, a estabilidade institucional ou a continuidade do Poder Nacional. Além de proteger seus próprios interesses, esses Estados exercem influência sobre a governança global do ciberespaço, estabelecem padrões tecnológicos internacionais e projetam poder informacional em escala global. Sob a perspectiva da Teoria da Profundidade Estratégica Cibernética, esta categoria representa o estágio

máximo de maturidade estratégica alcançável na Era Informacional.

Os intervalos de classificação do Índice de Profundidade Estratégica Cibernética (IPEC) foram definidos de modo a representar seis estágios sucessivos de maturidade da profundidade estratégica cibernética dos Estados, refletindo diferentes níveis de autonomia tecnológica, resiliência informacional e capacidade de preservação da soberania cibernética:

- Condição Crítica (-10 a 14,9);
- Profundidade Estratégica Muito Baixa (15 a 29,9);
- Profundidade Estratégica Baixa (30 a 44,9);
- Profundidade Estratégica Média (45 a 59,9);
- Profundidade Estratégica Alta (60 a 74,9); e
- Profundidade Estratégica Muito Alta (75 a 90).

A definição dessas faixas decorre diretamente da formulação matemática do IPEC e dos pressupostos centrais da Teoria da Profundidade Estratégica Cibernética (TPEC). Como o índice atribui pesos equivalentes às capacidades física, lógica e cognitiva e incorpora a dependência tecnológica externa como fator redutor, sua estrutura busca refletir o equilíbrio entre autonomia, resiliência e vulnerabilidade no ecossistema cibernético nacional.

A existência de uma faixa crítica inferior permite identificar Estados cuja dependência tecnológica e fragilidade estrutural

comprometem significativamente sua capacidade de garantir a continuidade das funções essenciais do Poder Nacional. Em sentido oposto, a faixa superior representa Estados capazes de construir elevados níveis de autonomia tecnológica, proteção de infraestruturas críticas, resiliência institucional e defesa cognitiva.

A limitação da categoria superior ao intervalo de 75 a 90 pontos decorre da própria arquitetura do índice. Considerando que a dependência tecnológica exerce influência negativa sobre o resultado final e que a obtenção de elevados níveis simultâneos de capacidade física, lógica e cognitiva constitui condição rara no sistema internacional, os valores máximos tornam-se naturalmente mais difíceis de alcançar.

Essa característica preserva o poder discriminatório do IPEC e aumenta sua aderência à distribuição real das capacidades cibernéticas observadas entre os Estados contemporâneos. Consequentemente, a classificação deixa de representar uma simples escala quantitativa e passa a constituir uma tipologia estratégica de maturidade cibernética, capaz de expressar diferentes estágios de desenvolvimento da soberania cibernética e da profundidade estratégica cibernética.

Dessa forma, a escala proposta converte-se em um componente analítico da própria TPEC, permitindo interpretar comparativamente o posicionamento dos Estados no ambiente informacional contemporâneo e avaliar sua capacidade de absorver, resistir, adaptar-se e recuperar-se de ameaças dirigidas às camadas física, lógica e cognitiva do ciberespaço.

Com o objetivo de fortalecer a validade empírica da teoria, o modelo será aplicado de forma comparativa aos casos dos Estados Unidos, China, Estônia, União Europeia e Brasil, utilizando os indicadores e procedimentos metodológicos estabelecidos pelo IPEC. A seleção desses casos busca contemplar diferentes níveis de desenvolvimento tecnológico, distintas estratégias de soberania digital e variados graus de autonomia cibernética, permitindo avaliar a capacidade explicativa da Teoria da Profundidade Estratégica Cibernética em contextos geopolíticos diversos.

a. ESTADOS UNIDOS

a.1 Capacidade Física (CF = 95)

Os Estados Unidos possuem a maior infraestrutura digital do mundo:

- Liderança em data centers;
- Infraestrutura energética robusta;
- Extensa rede de cabos submarinos;
- Sistema espacial avançado; e
- Proteção de infraestruturas críticas.

a.2 Capacidade Lógica (CL = 98)

Liderança global em:

- Inteligência Artificial;

- Computação em nuvem;
- Software;
- Semicondutores; e
- Plataformas digitais globais.

Empresas como *Google*, *Microsoft*, *Amazon*, *Apple*, *Meta* e *Nvidia* representam ativos estratégicos nacionais.

a.3 Capacidade Cognitiva (CC = 80)

Pontos fortes:

- Excelência universitária;
- Elevada produção científica; e
- Forte cultura de inovação.

Pontos fracos:

- Polarização política; e
- Elevada exposição à desinformação.

a.4 Dependência Tecnológica (DT = 15)

- Baixa dependência externa.

Os EUA controlam grande parte das tecnologias críticas globais.

Resultado: IPEC = (0,30×95) + (0,30×98) + (0,30×80) − (0,10×15) = 80,4

Classificação: Profundidade Estratégica Cibernética Muito Alta.

Os Estados Unidos situam-se na categoria de Potência Cibernética Consolidada, caracterizada por:

- Elevada autonomia tecnológica;
- Domínio das principais tecnologias críticas globais;
- Liderança em inteligência artificial, semicondutores e computação em nuvem;
- Forte capacidade de inovação;
- Ampla resiliência das infraestruturas digitais;
- Elevada capacidade de projeção de poder informacional.

O principal fator limitador para uma pontuação ainda maior é a dimensão cognitiva (CC = 80), impactada pela polarização política interna, pela fragmentação informacional e pela crescente exposição a campanhas de desinformação. Apesar disso, o país mantém uma das maiores profundidades estratégicas cibernéticas do sistema internacional.

b. CHINA

b.1 Capacidade Física (CF = 90)

A China realizou investimentos maciços em:

- Infraestrutura digital;
- Redes 5G;
- Satélites;
- Data centers; e
- Energia.

b.2 Capacidade Lógica (CL = 92)

Possui:

- Plataformas nacionais (*Alibaba, Tencent, Baidu*);
- Ecossistema de IA;
- Crescente produção de semicondutores; e
- Sistemas próprios de pagamento digital.

b.3 Capacidade Cognitiva (CC = 78)

Fortes mecanismos de coordenação estatal, com menor vulnerabilidade a campanhas externas de influência.

b.4 Dependência Tecnológica (DT = 20)

Embora tenha reduzido significativamente sua dependência, ainda enfrenta limitações em:

- Semicondutores avançados; e

- Litografia de ponta.

Resultado: IPEC = (0,30×90) + (0,30×92) + (0,30×78) − (0,10×20) = 76,0

Classificação: Profundidade Estratégica Cibernética Muito Alta.

A China enquadra-se na categoria de Potência Cibernética Consolidada, apresentando elevada profundidade estratégica cibernética em razão de:

- Ampla infraestrutura digital e energética;
- Liderança mundial em redes 5G;
- Forte capacidade espacial;
- Ecossistema tecnológico nacional robusto;
- Plataformas digitais próprias;
- Crescente autonomia em inteligência artificial;
- Sistemas financeiros digitais soberanos;
- Elevada coordenação estatal das políticas tecnológicas.

O principal fator limitador da pontuação chinesa permanece associado à dependência residual de tecnologias críticas de ponta, especialmente na produção de semicondutores avançados e equipamentos de litografia, segmentos ainda sujeitos a restrições tecnológicas externas.

Mesmo assim, a China demonstra elevado grau de autonomia estratégica e capacidade de absorção de choques tecnológicos, posicionando-se como uma das principais potências cibernéticas do sistema internacional.

c. ESTÔNIA

c.1 Capacidade Física (CF = 82)

Apesar do pequeno território, apresenta:

- Infraestrutura digital altamente integrada;
- Elevada conectividade; e
- Sistemas governamentais distribuídos.

c.2 Capacidade Lógica (CL = 80)

Possui:

- Identidade digital nacional;
- Interoperabilidade governamental; e
- Governo digital avançado.

c.3 Capacidade Cognitiva (CC = 92)

Constitui sua principal força estratégica, sendo consolidada após os ataques de 2007, fundamentada em:

- Educação digital;

- Cultura de segurança cibernética; e
- Defesa cognitiva.

c.4 Dependência Tecnológica (DT = 35)

Continua dependente de tecnologias produzidas fora do país.

Resultado: IPEC = (0,30×82) + (0,30×80) + (0,30×92) − (0,10×35) = 72,7

Classificação: Profundidade Estratégica Cibernética Alta.

A Estônia constitui um caso singular na aplicação da Teoria da Profundidade Estratégica Cibernética. Apesar de sua reduzida dimensão territorial e limitada capacidade material quando comparada às grandes potências, o país desenvolveu um dos ecossistemas digitais mais resilientes do mundo.

Sua principal vantagem estratégica encontra-se na Capacidade Cognitiva (CC = 92), a maior entre os casos analisados até o momento. Os ataques cibernéticos sofridos em 2007 impulsionaram a construção de uma cultura nacional de segurança cibernética baseada em:

- Educação digital abrangente;
- Elevada confiança institucional;
- Mecanismos de defesa cognitiva;
- Treinamento permanente da população;

  Integração entre governo, sociedade e setor privado.

Na dimensão lógica, a Estônia destaca-se pela identidade digital nacional, interoperabilidade entre sistemas governamentais e ampla digitalização dos serviços públicos. Na dimensão física, apresenta infraestrutura altamente conectada e distribuída, embora em escala inferior à das grandes potências.

O principal fator limitador do índice permanece sendo a dependência tecnológica externa (DT = 35), especialmente em relação a hardware avançado, semicondutores e parte das plataformas tecnológicas globais.

d. UNIÃO EUROPEIA

d.1 Capacidade Física (CF = 85)

A UE possui:

- Infraestrutura digital avançada;
- Elevada conectividade; e
- Sistemas energéticos modernos.

d.2 Capacidade Lógica (CL = 75)

Apesar da elevada capacidade científica, possui:

- Poucas plataformas digitais globais;
- Dependência tecnológica dos EUA; e
- Crescente dependência de IA estrangeira.

d.3 Capacidade Cognitiva (CC = 80)

Elevados níveis de:

- Educação;
- Confiança institucional; e
- Combate à desinformação.

d.4 Dependência Tecnológica (DT = 40)

Dependência moderada em:

- Nuvem;
- IA;
- Plataformas digitais.

Resultado: IPEC = (0,30×85) + (0,30×75) + (0,30×80) − (0,10×40) = 68,0

Classificação: Profundidade Estratégica Cibernética Alta.

A União Europeia apresenta elevada profundidade estratégica cibernética, sustentada por uma infraestrutura física robusta, altos níveis educacionais e um arcabouço regulatório avançado voltado para a proteção de dados, segurança digital e combate à desinformação.

Sua principal força reside na combinação entre:

- Elevada conectividade digital;

- Infraestrutura energética moderna;
- Forte capacidade científica;
- Instituições estáveis;
- Políticas de proteção do ambiente informacional.

Na dimensão cognitiva, a União Europeia mantém elevados níveis de alfabetização digital, confiança institucional e mecanismos de enfrentamento à desinformação, fatores que contribuem para sua resiliência social e política.

Entretanto, sua principal vulnerabilidade encontra-se na dimensão lógica. Apesar da excelência científica e tecnológica, a União Europeia possui limitada presença entre as grandes plataformas digitais globais e mantém dependência significativa de tecnologias desenvolvidas principalmente pelos Estados Unidos. Essa dependência manifesta-se em áreas estratégicas como:

- Computação em nuvem;
- Inteligência artificial;
- Sistemas operacionais;
- Plataformas digitais;
- Serviços digitais de grande escala.

Consequentemente, a Dependência Tecnológica Externa (DT = 40) reduz significativamente sua profundidade estratégica cibernética.

e. BRASIL

e.1 Capacidade Física (CF = 70)

Pontos fortes:

- Sistema financeiro digital robusto;
- PIX;
- GOV.BR; e
- Matriz energética favorável.

Pontos fracos:

- Concentração de infraestrutura crítica; e
- Dependência tecnológica.

e.2 Capacidade Lógica (CL = 55)

Principais limitações:

- Baixa produção de semicondutores;
- Reduzida presença em IA avançada; e
- Ausência de plataformas digitais globais.

e.3 Capacidade Cognitiva (CC = 68)

Pontos fortes:

- Expansão da inclusão digital; e
- Capacidade acadêmica relevante.

Pontos fracos:

- Elevada exposição à desinformação; e
- Baixa institucionalização da defesa cognitiva.

e.4 Dependência Tecnológica (DT = 70)

Elevada dependência em:

- Nuvem;
- IA;
- Semicondutores;
- Plataformas digitais.

Resultado: IPEC = (0,30×70) + (0,30×55) + (0,30×68) − (0,10×70) = 50,9

Classificação: Profundidade Estratégica Cibernética Média

O Brasil apresenta uma profundidade estratégica cibernética intermediária, situando-se na categoria de Estados em processo de consolidação de capacidades estratégicas. O resultado demonstra que o país possui ativos relevantes para a construção da soberania cibernética, mas ainda enfrenta limitações estruturais que restringem sua autonomia tecnológica.

Na dimensão física, destacam-se:

- Sistema financeiro digital nacional;
- Ecossistema PIX;
- A plataforma GOV.BR;
- Ampla matriz energética renovável;
- Crescente infraestrutura de conectividade.

Esses elementos fornecem uma base importante para a resiliência do ecossistema digital brasileiro.

Na dimensão lógica, contudo, encontram-se as principais limitações. O país apresenta:

- Baixa capacidade de produção de semicondutores;
- Reduzida participação na corrida global da inteligência artificial;
- Ausência de plataformas digitais globais;
- Dependência significativa de software e infraestrutura tecnológica estrangeira.

Na dimensão cognitiva, o Brasil possui uma comunidade acadêmica relevante e crescente inclusão digital, mas enfrenta desafios relacionados à disseminação de desinformação, polarização social e limitada institucionalização de políticas permanentes de defesa cognitiva.

O principal fator redutor do índice é a elevada Dependência Tecnológica Externa (DT = 70), uma das maiores entre os casos analisados. Essa dependência manifesta-se em setores estratégicos como:

- Computação em nuvem;
- Inteligência artificial;
- Semicondutores;
- Sistemas operacionais;
- Plataformas digitais globais.

6.5. Análise Comparativa dos Resultados do IPEC

A aplicação do Índice de Profundidade Estratégica Cibernética (IPEC) aos Estados Unidos, China, Estônia, União Europeia e Brasil permite identificar padrões estruturais relevantes para a compreensão da distribuição de poder na Era Informacional. Sob a perspectiva da Teoria da Profundidade Estratégica Cibernética (TPEC), os resultados sugerem que a competição estratégica contemporânea está sendo progressivamente deslocada da geografia física para a geografia informacional, na qual a autonomia tecnológica, a resiliência institucional e a defesa cognitiva assumem papel central na preservação da soberania e da capacidade de defesa dos Estados.

A análise revela que a principal variável explicativa das diferenças observadas não é a dimensão territorial nem a população, mas a capacidade de controlar tecnologias críticas e reduzir dependências

externas. Em todos os casos avaliados, os maiores níveis de profundidade estratégica estão associados à elevada autonomia tecnológica e à existência de mecanismos robustos de defesa cognitiva.

Os Estados Unidos ocupam a primeira posição no ranking do IPEC, refletindo sua condição de principal potência tecnológica do sistema internacional. Sua vantagem estratégica decorre do domínio da camada lógica do ciberespaço, sustentado por empresas líderes em inteligência artificial, semicondutores, computação em nuvem e plataformas digitais globais.

A principal vulnerabilidade identificada encontra-se na crescente polarização política interna e na ampliação da superfície de exposição a operações de influência e desinformação.

Fruto da análise dos conhecimentos gerados emprego do IPEC, recomenda-se os seguintes aspectos nas políticas pública dos EUA:

- Fortalecer programas nacionais de defesa cognitiva;
- Ampliar mecanismos de proteção contra operações de influência estrangeira;
- Reforçar a segurança das cadeias de suprimentos de semicondutores;
- Expandir investimentos em computação quântica e inteligência artificial avançada;
- Aumentar a proteção das infraestruturas críticas contra ataques híbridos; e

- Promover maior integração entre segurança nacional, setor privado e comunidade científica.

Em relação a China, ela consolidou-se como principal desafiante estratégico dos Estados Unidos no domínio cibernético. Seus investimentos em infraestrutura digital, inteligência artificial, sistemas financeiros digitais e produção tecnológica ampliaram significativamente sua profundidade estratégica.

Sua principal vulnerabilidade permanece associada à dependência residual de tecnologias críticas relacionadas à produção de semicondutores avançados e equipamentos de litografia.

Recomendações para aperfeiçoamento das políticas públicas do setor:

- Acelerar a autossuficiência em semicondutores de última geração;
- Ampliar investimentos em pesquisa básica e inovação disruptiva;
- Reduzir vulnerabilidades em cadeias globais de suprimentos estratégicos;
- Fortalecer mecanismos de proteção contra sabotagem tecnológica;
- Expandir programas de formação de especialistas em tecnologias críticas; e
- Consolidar ecossistemas nacionais de inteligência artificial.

No tocante a Estônia, o país representa o caso mais eficiente de conversão de recursos limitados em elevada profundidade estratégica cibernética. Sua principal vantagem decorre da combinação entre governança digital avançada, elevada alfabetização digital e forte cultura de segurança cibernética.

Sua vulnerabilidade estrutural está relacionada à limitada escala econômica e à dependência tecnológica externa para determinados componentes estratégicos.

Recomendações voltadas às políticas públicas do setor:

- Manter programas permanentes de educação digital e defesa cognitiva;
- Ampliar a redundância de infraestruturas digitais críticas;
- Fortalecer parcerias estratégicas no âmbito da OTAN e da União Europeia;
- Expandir capacidades nacionais de ciberdefesa;
- Desenvolver mecanismos de continuidade governamental em ambientes de crise; e
- Investir em tecnologias emergentes para reduzir dependências externas.

A União Europeia apresenta elevada profundidade estratégica nas dimensões física e cognitiva, porém enfrenta limitações relevantes na camada lógica devido à dependência de plataformas digitais,

serviços de nuvem e inteligência artificial predominantemente controlados por atores externos.

Sua principal vulnerabilidade é a assimetria entre capacidade regulatória e capacidade tecnológica.

Recomendações direcionadas às políticas públicas do setor:

- Acelerar a implementação de programas de soberania digital europeia;
- Ampliar investimentos em inteligência artificial própria;
- Fortalecer iniciativas de computação em nuvem soberana;
- Incentivar a criação de plataformas digitais europeias competitivas;
- Desenvolver capacidade industrial avançada em semicondutores; e
- Ampliar mecanismos coordenados de defesa cognitiva e combate à desinformação.

O Brasil apresenta uma posição intermediária, refletindo a coexistência de importantes capacidades nacionais e elevada dependência tecnológica externa. O país possui ativos estratégicos relevantes, como o PIX, o GOV.BR e uma infraestrutura financeira digital avançada, mas ainda demonstra limitações significativas na camada lógica do ciberespaço.

Sua principal vulnerabilidade reside na dependência de semicondutores, inteligência artificial, plataformas digitais globais e serviços de computação em nuvem.

Recomendações para aperfeiçoamento das políticas públicas do setor:

- Elaborar uma Estratégia Nacional de Profundidade Estratégica Cibernética;
- Estabelecer uma Política Nacional de Autonomia Tecnológica;
- Ampliar investimentos em inteligência artificial e computação avançada;
- Desenvolver capacidade nacional de semicondutores;
- Fortalecer ecossistemas de inovação e startups tecnológicas;
- Criar uma Estratégia Nacional de Defesa Cognitiva;
- Institucionalizar programas permanentes de alfabetização digital;
- Ampliar a proteção das infraestruturas críticas nacionais;
- Fortalecer a integração entre governo, academia, indústria e setor de defesa; e
- Expandir programas de formação de recursos humanos em áreas STEM.

Os resultados indicam que o sistema internacional está evoluindo para uma estrutura de poder baseada em três elementos centrais:

a. Autonomia tecnológica – capacidade de desenvolver e controlar tecnologias críticas;

b. Resiliência institucional – capacidade de absorver e recuperar-se de choques sistêmicos;

c. Defesa cognitiva – capacidade de proteger a sociedade contra operações de influência e manipulação informacional.

Nesse contexto, a competição internacional tende a deslocar-se progressivamente para setores como inteligência artificial, computação quântica, semicondutores, sistemas autônomos e controle dos fluxos globais de informação.

A análise comparativa sugere que os Estados que conseguirem integrar essas capacidades em uma estratégia nacional coerente possuirão maiores níveis de profundidade estratégica cibernética e, consequentemente, maior capacidade de preservar sua soberania, sua liberdade de ação e sua capacidade de defesa diante das transformações da Era Informacional.

6.6. Potencial Científico do IPEC

O Índice de Profundidade Estratégica Cibernética (IPEC) representa uma das principais contribuições da Teoria da Profundidade Estratégica Cibernética (TPEC), ao fornecer um mecanismo de operacionalização capaz de transformar um construto teórico em objeto de observação, mensuração e comparação sistemática.

A relevância científica do IPEC decorre do fato de que ele permite estabelecer uma ponte metodológica entre teoria e evidência empírica. Enquanto a TPEC oferece um modelo explicativo para compreender a sobrevivência estratégica dos Estados na Era Informacional, o IPEC fornece os instrumentos necessários para avaliar empiricamente a validade desse modelo.

Sob essa perspectiva, o índice não deve ser compreendido apenas como uma ferramenta de classificação, mas como um instrumento analítico destinado à produção de conhecimento científico sobre a distribuição internacional de capacidades cibernéticas e informacionais.

Assim, o IPEC possui as seguintes contribuições científicas:

- Permitir a operacionalização da Profundidade Estratégica Cibernética como variável observável: Historicamente, conceitos como poder nacional, soberania e autonomia estratégica foram frequentemente utilizados de forma abstrata, dificultando sua mensuração objetiva. O IPEC busca superar essa limitação ao decompor a profundidade estratégica cibernética em dimensões específicas — física, lógica, cognitiva e dependência tecnológica — associadas a indicadores empíricos passíveis de observação.

Dessa forma, o índice transforma uma categoria teórica em uma variável mensurável, permitindo que diferentes Estados sejam avaliados segundo critérios comuns e comparáveis.

Essa característica aproxima a TPEC de outras tradições consolidadas das Relações Internacionais, como os índices de poder

nacional, os indicadores de governança e os modelos de capacidade estatal utilizados na literatura comparada.

- Possibilidade de testar empiricamente as hipóteses derivadas da TPEC: Uma teoria científica somente adquire robustez quando suas proposições podem ser confrontadas com evidências observáveis. O IPEC permite verificar, por exemplo, se Estados com maior profundidade estratégica cibernética apresentam efetivamente maiores níveis de resiliência diante de ataques cibernéticos, crises tecnológicas, campanhas de desinformação ou interrupções em infraestruturas críticas.

Da mesma forma, possibilita examinar se elevados níveis de dependência tecnológica estão associados a maiores graus de vulnerabilidade estratégica, conforme previsto pela teoria.

Ao permitir a comparação entre expectativas teóricas e resultados observados, o índice cria condições para a validação, refutação ou refinamento da própria TPEC, fortalecendo seu caráter científico.

- Criação de um instrumento comparativo aplicável a diferentes contextos nacionais: O IPEC permite avaliar como os Estados se posicionam na competição estratégica da Era Informacional, identificando diferenças de capacidade entre potências tecnológicas, economias emergentes e países em desenvolvimento.

A aplicação sistemática do índice possibilita a construção de rankings internacionais, análises regionais e estudos longitudinais capazes de revelar padrões de distribuição de poder no ambiente digital.

Sob essa perspectiva, o IPEC contribui para o desenvolvimento de uma nova agenda de pesquisa em Geopolítica Digital, permitindo compreender como capacidades cibernéticas influenciam a estrutura de poder do sistema internacional contemporâneo.

Além disso, a utilização do índice em séries temporais poderá revelar tendências de ascensão, estagnação ou declínio da profundidade estratégica cibernética dos Estados ao longo do tempo.

- Capacidade de integrar diferentes tradições teóricas frequentemente tratadas de forma isolada: A literatura sobre soberania digital concentra-se predominantemente na autonomia tecnológica. Os estudos sobre poder nacional enfatizam recursos materiais e capacidades estatais. As pesquisas sobre resiliência analisam a capacidade de recuperação diante de crises. Já os estudos sobre ciberpoder investigam a capacidade de produzir efeitos estratégicos no ambiente digital.

O IPEC oferece uma estrutura analítica capaz de integrar essas abordagens em um único modelo explicativo.

Nesse sentido, o índice pode contribuir para o desenvolvimento de uma nova geração de estudos interdisciplinares situados na intersecção entre Relações Internacionais, Estudos Estratégicos, Segurança Cibernética, Economia Política Internacional e Governança Digital.

Em pesquisas futuras, o índice poderá ser utilizado em análises estatísticas multivariadas destinadas a investigar a relação entre profundidade estratégica cibernética e variáveis como crescimento

econômico, inovação tecnológica, estabilidade institucional, competitividade internacional e capacidade de projeção de poder.

Da mesma forma, poderá ser empregado em estudos de correlação e causalidade envolvendo indicadores de desenvolvimento digital, segurança cibernética, soberania tecnológica e resiliência nacional.

A utilização de técnicas como Análise Fatorial Exploratória, Análise Fatorial Confirmatória, Modelagem de Equações Estruturais e Painéis Longitudinais permitirá aperfeiçoar os pesos das variáveis e testar a consistência interna do índice em diferentes contextos empíricos.

Esses procedimentos contribuirão para transformar o IPEC de um instrumento inicialmente teórico em uma ferramenta consolidada de análise estratégica internacional.

7. ESTUDO DE CASO: O BRASIL E A PROFUNDIDADE ESTRATÉGICA CIBERNÉTICA

7.1. O Brasil na Era Informacional

Nas últimas duas décadas, o Brasil experimentou um acelerado processo de transformação digital. A expansão da conectividade, a digitalização dos serviços públicos, a modernização do sistema financeiro e a crescente adoção de tecnologias digitais pela sociedade produziram uma profunda reconfiguração do ambiente estratégico nacional.

Sob a perspectiva da Teoria da Profundidade Estratégica Cibernética, o Brasil apresenta características particularmente relevantes para análise.

Por um lado, possui um dos maiores mercados digitais do mundo, ampla infraestrutura financeira e crescente capacidade científica e tecnológica. Por outro lado, mantém elevado grau de dependência tecnológica externa em setores considerados críticos para a soberania nacional.

Essa combinação torna o Brasil um caso particularmente adequado para examinar os mecanismos propostos pela TPEC.

7.2. O PIX Como Infraestrutura Estratégica Nacional

O PIX representa uma das mais relevantes inovações institucionais e tecnológicas da história recente do Brasil.

Lançado pelo Banco Central em 2020, o sistema transformou profundamente a dinâmica dos pagamentos eletrônicos nacionais, tornando-se rapidamente a principal infraestrutura de transações financeiras do país.

Sob a perspectiva tradicional, o PIX poderia ser interpretado apenas como uma plataforma de pagamentos. Entretanto, sob a ótica da Profundidade Estratégica Cibernética, sua relevância é muito maior.

O sistema constitui uma infraestrutura crítica nacional. Sua interrupção prolongada produziria impactos imediatos sobre:

- Atividade econômica;
- Arrecadação tributária;
- Sistema bancário;

- Comércio eletrônico;
- Serviços públicos; e
- Estabilidade social.

O PIX representa um exemplo concreto de ativo pertencente à Amazônia Cibernética brasileira.

Sua importância estratégica decorre não apenas do volume de recursos movimentados, mas de sua centralidade para o funcionamento da economia nacional. Nesse sentido, sua proteção constitui questão diretamente relacionada à soberania nacional.

7.3. A Dimensão Física da Profundidade Estratégica Brasileira

A análise da dimensão física brasileira revela avanços significativos. O país possui:

- ampla rede de telecomunicações;
- múltiplos cabos submarinos internacionais;
- grande capacidade de geração energética;
- crescente número de centros de dados; e
- sistemas financeiros altamente digitalizados.

A infraestrutura que sustenta o PIX demonstra elevado grau de robustez operacional. Mesmo diante de picos de utilização, o sistema manteve níveis elevados de disponibilidade.

Esse desempenho sugere a existência de razoável profundidade estratégica na camada física. Entretanto, permanecem vulnerabilidades relevantes.

A concentração de parte significativa da infraestrutura de computação em provedores estrangeiros de nuvem reduz a autonomia nacional. Além disso, a dependência de equipamentos produzidos no exterior limita a capacidade de resposta em cenários de interrupção das cadeias globais de suprimento.

Sob a ótica da TPEC, essas vulnerabilidades reduzem a profundidade estratégica física do país.

7.4. A Dimensão Lógica e a Dependência Tecnológica

A camada lógica constitui o principal desafio brasileiro. Embora o país possua capacidade relevante de desenvolvimento de software e ecossistema tecnológico dinâmico, observa-se elevada dependência de tecnologias estrangeiras.

Grande parte dos sistemas operacionais utilizados em infraestruturas críticas nacionais é desenvolvida no exterior. Os principais provedores de computação em nuvem pertencem a empresas estrangeiras. Os modelos de inteligência artificial mais avançados também são predominantemente produzidos fora do país.

Essa realidade cria vulnerabilidades estratégicas. Em situações de crise internacional, sanções econômicas ou restrições tecnológicas, a continuidade de serviços essenciais pode ser comprometida.

O caso dos semicondutores é particularmente ilustrativo, na medida em que a economia digital contemporânea depende fortemente desses componentes. Entretanto, o Brasil possui participação limitada em sua cadeia global de produção.

A dependência tecnológica torna-se, portanto, um fator estrutural de vulnerabilidade.

Assim, a teoria proposta sustenta que essa dependência reduz diretamente a profundidade estratégica cibernética brasileira.

Um dos episódios mais relevantes para a validação da teoria ocorreu quando vulnerabilidades em fornecedores conectados ao Sistema Financeiro Nacional demonstraram a importância estratégica da cadeia de suprimentos digital.

O episódio evidenciou que a robustez de uma infraestrutura não depende apenas de seus sistemas centrais. Ela depende também da segurança dos atores periféricos integrados ao ecossistema.

Sob a ótica da TPEC, esse caso revela um mecanismo causal importante. A existência de profundidade estratégica não pode ser avaliada apenas pela proteção dos ativos centrais. Ela depende da capacidade de proteger toda a rede de interdependências que sustenta o funcionamento do sistema.

O incidente demonstrou que vulnerabilidades em fornecedores externos podem comprometer ativos considerados críticos. Consequentemente, a profundidade estratégica deve ser compreendida como atributo sistêmico e não apenas setorial.

7.5. A Dimensão Cognitiva e a Guerra Informacional

A dimensão cognitiva representa a contribuição mais inovadora da teoria proposta.

No caso brasileiro, essa dimensão revelou-se particularmente relevante durante episódios recentes de desinformação relacionados a infraestruturas digitais.

As campanhas envolvendo narrativas falsas sobre o PIX demonstraram que operações cognitivas podem produzir efeitos estratégicos sem comprometer qualquer componente físico ou lógico do sistema. Nenhum servidor foi destruído, nenhuma rede foi interrompida e nenhum software foi comprometido. Contudo, observou-se impacto sobre a confiança pública.

Esse episódio confirma um dos pressupostos centrais da TPEC: Na Era Informacional, a confiança tornou-se infraestrutura estratégica.

A estabilidade de sistemas digitais depende não apenas de sua segurança tecnológica, mas também da percepção de legitimidade e confiabilidade construída junto à população.

A profundidade cognitiva corresponde precisamente à capacidade de preservar essa confiança diante de campanhas de manipulação informacional.

Outro exemplo relevante é a plataforma GOV.BR. A iniciativa consolidou milhares de serviços públicos em um ambiente digital unificado, ampliando significativamente a eficiência administrativa.

Sob a perspectiva da TPEC, o GOV.BR representa simultaneamente uma oportunidade e um desafio.

A centralização digital aumenta a eficiência operacional. Entretanto, também amplia a importância estratégica da plataforma.

Quanto maior a dependência de um único sistema, maior a necessidade de mecanismos de redundância, proteção e continuidade operacional.

A existência de planos de contingência, sistemas alternativos e protocolos de recuperação torna-se elemento fundamental da profundidade estratégica.

O caso evidencia que a digitalização estatal precisa ser acompanhada pela construção de mecanismos de resiliência.

7.6. Discussão dos Resultados Brasileiros

A análise do caso brasileiro confirma os principais mecanismos previstos pela Teoria da Profundidade Estratégica Cibernética.

Primeiramente, demonstra que a sobrevivência estratégica contemporânea depende de capacidades distribuídas entre diferentes camadas do espaço cibernético. Em segundo lugar, evidencia que a dependência tecnológica constitui fator limitador da autonomia nacional. Por fim, confirma que a dimensão cognitiva se tornou componente indispensável da segurança estratégica.

O caso brasileiro sugere que os maiores desafios para a construção de profundidade estratégica cibernética não estão necessariamente na infraestrutura física, mas no fortalecimento da autonomia tecnológica e da resiliência cognitiva.

Esses resultados oferecem evidências preliminares favoráveis à hipótese central da pesquisa e demonstram a aplicabilidade da TPEC como instrumento de análise da soberania e da sobrevivência estratégica na Era Informacional.

8. DISCUSSÃO

Os resultados obtidos ao longo desta investigação sugerem que a transformação digital das sociedades produziu uma mudança estrutural nos fundamentos da sobrevivência estratégica dos Estados. Embora os princípios formulados pela Geopolítica clássica permaneçam relevantes, a análise desenvolvida indica que a capacidade de absorver ameaças deixou de depender exclusivamente da profundidade territorial e passou a envolver crescentemente a profundidade dos ecossistemas informacionais nacionais.

Historicamente, a profundidade estratégica esteve associada à geografia. A sobrevivência estatal era favorecida pela existência de vastos territórios, barreiras naturais e capacidade de dispersão dos centros de poder. Essa lógica permaneceu válida durante grande parte da história moderna e influenciou profundamente o pensamento estratégico ocidental.

Entretanto, os casos analisados demonstram que a distância física deixou de constituir proteção suficiente diante das ameaças contemporâneas.

Um ataque cibernético direcionado a sistemas financeiros, redes elétricas ou infraestruturas governamentais pode produzir efeitos imediatos, independentemente da localização geográfica do agressor.

Nesse contexto, a Teoria da Profundidade Estratégica Cibernética não substitui a Geopolítica clássica. Ao contrário, amplia seus pressupostos para um ambiente caracterizado pela crescente centralidade da informação.

A principal contribuição da teoria consiste em deslocar o conceito de profundidade estratégica do espaço físico para o espaço funcional. A questão estratégica fundamental deixa de ser:

"Qual a distância entre a ameaça e o centro de poder?" e passa a ser: "Quantas camadas de proteção, autonomia, redundância e resiliência existem entre a ameaça e a capacidade de produzir danos sistêmicos?"

Essa mudança representa uma ampliação conceitual significativa da teoria clássica da profundidade estratégica.

Outro resultado relevante da pesquisa refere-se à integração entre as literaturas de soberania cibernética e resiliência nacional.

A revisão sistemática demonstrou que essas duas correntes teóricas evoluíram de forma relativamente independente.

A literatura sobre soberania cibernética concentrou-se na capacidade estatal de controlar as camadas física, lógica e cognitiva do espaço cibernético. Por sua vez, os estudos sobre resiliência nacional enfatizaram a capacidade dos sistemas de absorver e recuperar-se de choques.

A análise desenvolvida neste artigo sugere que essas duas perspectivas são complementares.

A soberania sem profundidade estratégica produz sistemas vulneráveis. Da mesma forma, a resiliência sem autonomia tecnológica tende a apresentar limitações estruturais.

A TPEC propõe precisamente a integração desses dois campos. Sob essa perspectiva, a profundidade estratégica cibernética pode ser compreendida como o mecanismo que conecta soberania e resiliência.

Quanto maior a profundidade existente nas camadas física, lógica e cognitiva, maior a capacidade de preservação da soberania diante de crises e ataques.

Essa interpretação amplia a compreensão tradicional da segurança nacional e oferece uma abordagem mais adequada às características da Era Informacional.

Outro ponto relevante é que os resultados da pesquisa indicam que a principal inovação teórica da TPEC reside na incorporação da dimensão cognitiva como componente estruturante da profundidade estratégica.

Historicamente, os estudos estratégicos concentraram-se predominantemente em recursos materiais. O território, população, recursos naturais, capacidade industrial e poder militar constituíram os principais indicadores utilizados para avaliar a posição relativa dos Estados.

A análise dos casos contemporâneos sugere que essa abordagem se tornou insuficiente. Os episódios envolvendo campanhas de desinformação, operações de influência e guerra cognitiva

demonstram que a disputa estratégica contemporânea ocorre crescentemente no domínio das percepções.

A estabilidade de sistemas digitais depende não apenas de sua robustez tecnológica, mas também da confiança social que sustenta seu funcionamento.

O caso brasileiro envolvendo narrativas falsas relacionadas ao PIX ilustra esse fenômeno. Nenhuma infraestrutura foi fisicamente atacada, nenhum sistema lógico foi comprometido. Mesmo assim, observou-se impacto estratégico decorrente da tentativa de influenciar percepções coletivas.

Esse fenômeno sugere que a confiança tornou-se um recurso estratégico.

Consequentemente, a capacidade de preservar a integridade do ambiente cognitivo emerge como elemento central da soberania contemporânea. A TPEC propõe que a profundidade cognitiva constitua uma forma específica de profundidade estratégica.

Essa formulação representa uma contribuição original à literatura internacional sobre segurança e soberania digital.

A análise comparativa internacional revelou que a dependência tecnológica constitui um dos principais fatores explicativos das diferenças observadas entre os níveis de profundidade estratégica informacional.

Os casos dos Estados Unidos e da China demonstram que elevados níveis de autonomia tecnológica tendem a produzir maiores níveis de profundidade estratégica.

Por outro lado, os casos da União Europeia e do Brasil evidenciam os desafios associados à dependência de plataformas, semicondutores, serviços de nuvem e sistemas de inteligência artificial desenvolvidos externamente.

Esse resultado confirma uma das hipóteses centrais da teoria. Na Era Informacional, a dependência tecnológica exerce papel semelhante ao desempenhado pelas dependências energéticas ou logísticas em períodos anteriores. Ela cria vulnerabilidades que podem ser exploradas em contextos de competição geopolítica.

Consequentemente, a autonomia tecnológica emerge como componente essencial da sobrevivência estratégica.

A contribuição da TPEC consiste em incorporar explicitamente essa variável ao modelo analítico por meio do conceito de Dependência Tecnológica Externa (DT).

Essa inclusão permite compreender por que Estados com níveis semelhantes de desenvolvimento econômico podem apresentar capacidades distintas de resistência estratégica.

8.1. O IPEC e a Operacionalização da Teoria

Um dos desafios centrais enfrentados pelas teorias contemporâneas da soberania digital reside na dificuldade de transformar conceitos abstratos em instrumentos empiricamente verificáveis.

Nesse aspecto, o Índice de Profundidade Estratégica Cibernética representa uma contribuição metodológica relevante.

Ao operacionalizar as dimensões física, lógica, cognitiva e de dependência tecnológica, o índice permite converter a teoria em ferramenta analítica passível de comparação internacional.

Embora a aplicação realizada neste estudo possua caráter exploratório, os resultados sugerem que o IPEC apresenta potencial para futuras pesquisas quantitativas.

Sua utilização poderá permitir: comparações longitudinais; análises regionais; estudos de correlação; construção de rankings internacionais; e a avaliação de políticas públicas.

Dessa forma, a TPEC avança além da formulação conceitual e oferece mecanismos concretos para sua validação empírica.

A sua principal implicação teórica refere-se à necessidade de reformulação dos conceitos clássicos utilizados para compreender o poder e a soberania no século XXI.

A análise desenvolvida sugere que a sobrevivência estratégica dos Estados depende crescentemente da capacidade de construir profundidade em ambientes informacionais.

Essa constatação possui implicações para diferentes áreas do conhecimento.

Para a Geopolítica, significa reconhecer que o espaço digital se tornou componente permanente da competição internacional. Em relação aos Estudos Estratégicos, implica ampliar o conceito de profundidade estratégica para além da dimensão territorial. No seio da Segurança Nacional, exige-se incorporar a proteção de ecossistemas informacionais como objetivo estratégico prioritário.

Na formulação de políticas públicas, reforça a importância dos investimentos em autonomia tecnológica, educação digital e defesa cognitiva.

Nesse sentido, a TPEC oferece uma estrutura conceitual capaz de integrar essas diferentes dimensões em um único modelo explicativo.

Os resultados obtidos possuem importantes implicações para formuladores de políticas públicas.

A teoria sugere que a construção da soberania na Era Informacional exige políticas simultâneas em três frentes.

Fortalecimento da Camada Física: Os Estados devem ampliar a proteção de infraestruturas críticas; centros de dados; sistemas energéticos; redes de telecomunicações; e cabos submarinos. A redundância dessas infraestruturas torna-se elemento central da segurança nacional.

Fortalecimento da Camada Lógica: A redução da dependência tecnológica exige investimentos em pesquisa e desenvolvimento; fortalecimento da indústria nacional de software; desenvolvimento de inteligência artificial; e a ampliação da capacidade nacional em semicondutores. A autonomia tecnológica passa a representar questão estratégica de longo prazo.

Fortalecimento da Camada Cognitiva: Os resultados sugerem que programas de alfabetização digital; educação tecnológica; combate à desinformação; e defesa cognitiva devem ser incorporados às políticas nacionais de segurança. A proteção da sociedade contra

operações de influência passa a constituir componente da defesa nacional.

8.2. Limitações e Robustez da Teoria

Apesar dos resultados promissores, a teoria proposta apresenta limitações que devem ser reconhecidas.

Primeiramente, trata-se de uma formulação inicial que necessita de validação empírica ampliada.

A aplicação do IPEC foi realizada de forma exploratória e deverá ser refinada por meio da utilização de bases de dados internacionais padronizadas. Além disso, a rápida evolução tecnológica poderá exigir adaptações futuras do modelo.

Novas tecnologias, como computação quântica, inteligência artificial geral e sistemas autônomos avançados, poderão alterar significativamente a dinâmica da profundidade estratégica informacional. Entretanto, essas limitações não reduzem a relevância da contribuição apresentada. Ao contrário, indicam a existência de uma agenda de pesquisa ampla e promissora.

A capacidade da teoria de integrar conceitos provenientes da Geopolítica, da Soberania Cibernética, da Resiliência Nacional e da Segurança Digital sugere elevado potencial explicativo.

9. CONCLUSÕES

A transformação digital das sociedades contemporâneas produziu uma mudança estrutural nos fundamentos da soberania, da segurança nacional e da competição internacional. Ao longo da

história moderna, a capacidade de sobrevivência dos Estados esteve fortemente associada à geografia e à profundidade territorial. A extensão do território, a presença de barreiras naturais e a distância entre as fronteiras e os centros vitais de poder constituíam elementos centrais da segurança estratégica.

Entretanto, a consolidação da Era Informacional alterou profundamente essa realidade.

A crescente dependência de infraestruturas digitais, sistemas computacionais, inteligência artificial, plataformas tecnológicas e fluxos globais de informação reduziu a relevância relativa da distância geográfica e ampliou a importância dos ecossistemas informacionais como espaços centrais da disputa de poder.

Partindo desse contexto, a presente pesquisa buscou responder à seguinte questão:

Como os Estados preservam sua autonomia estratégica em um ambiente caracterizado pela crescente dependência digital e pela redução da relevância da distância geográfica?

A resposta proposta foi formulada por meio da Teoria da Profundidade Estratégica Cibernética (TPEC)

A teoria sustenta que a sobrevivência estratégica dos Estados no século XXI depende da capacidade de construir profundidade nas camadas física, lógica e cognitiva do espaço cibernético, reduzindo simultaneamente sua dependência tecnológica externa.

Essa formulação permitiu ampliar o conceito clássico de profundidade estratégica para além da dimensão territorial,

incorporando as especificidades da Era Informacional.

A pesquisa demonstrou que a literatura especializada apresenta importantes contribuições sobre Geopolítica, Resiliência Nacional, Poder Cibernético, Soberania Digital e Soberania Cibernética. Contudo, identificou-se uma lacuna teórica relacionada à ausência de um modelo capaz de explicar como os Estados constroem profundidade estratégica em seus ecossistemas informacionais.

A TPEC foi desenvolvida precisamente para preencher essa lacuna.

Do ponto de vista conceitual, a teoria definiu a profundidade estratégica informacional como a capacidade de um Estado absorver, resistir, adaptar-se e recuperar-se de ameaças dirigidas ao seu ecossistema informacional estratégico, preservando sua autonomia decisória, liberdade de ação e continuidade do exercício do Poder Nacional.

Essa definição permitiu deslocar o foco da análise estratégica do espaço geográfico para o espaço funcional.

Em vez de medir a segurança pela distância física entre ameaça e alvo, a teoria propõe avaliar a quantidade de camadas de proteção, redundância, autonomia e resiliência existentes entre uma ameaça e a capacidade de produzir danos sistêmicos.

A pesquisa também demonstrou que a profundidade estratégica contemporânea é construída sobre três dimensões fundamentais.

A primeira corresponde à camada física, composta pelas infraestruturas materiais que sustentam o funcionamento do espaço cibernético. A segunda refere-se à camada lógica, constituída pelos

sistemas, algoritmos, softwares e tecnologias responsáveis pelo processamento da informação. A terceira corresponde à camada cognitiva, representada pelas percepções, comportamentos, valores e processos decisórios que influenciam a estabilidade das sociedades contemporâneas.

Entre essas três dimensões, a pesquisa identificou a camada cognitiva como uma das principais inovações analíticas da teoria.

Os estudos de caso analisados demonstraram que os conflitos contemporâneos não se limitam à destruição de infraestruturas ou à interrupção de sistemas digitais. Crescentemente, eles buscam influenciar percepções, alterar comportamentos e comprometer a confiança pública.

Nesse contexto, a capacidade de resistir à manipulação informacional torna-se componente essencial da soberania.

Outra contribuição relevante da pesquisa foi a incorporação da Dependência Tecnológica Externa como variável explicativa central.

Os resultados obtidos indicam que a autonomia tecnológica constitui um dos principais determinantes da profundidade estratégica informacional.

Estados excessivamente dependentes de plataformas, semicondutores, sistemas operacionais, inteligência artificial ou serviços de computação em nuvem controlados por atores externos tendem a apresentar maior vulnerabilidade estratégica.

A análise comparativa dos casos dos Estados Unidos, China, Estônia, União Europeia e Brasil reforçou essa conclusão.

Os países que apresentam maiores níveis de autonomia tecnológica também tendem a apresentar maiores níveis de profundidade estratégica informacional.

No plano metodológico, a pesquisa procurou avançar além da formulação conceitual por meio da criação do Índice de Profundidade Estratégica Cibernética (IPEC).

Esse instrumento foi concebido para permitir a operacionalização empírica da teoria, transformando conceitos abstratos em variáveis passíveis de observação, comparação e mensuração.

Embora sua aplicação realizada neste estudo possua caráter exploratório, o IPEC oferece bases promissoras para futuras investigações quantitativas e comparativas.

O estudo de caso brasileiro demonstrou a utilidade prática da teoria.

A análise do ecossistema PIX, da plataforma GOV.BR e das iniciativas nacionais de segurança cibernética revelou que a profundidade estratégica contemporânea depende simultaneamente da robustez tecnológica, da autonomia digital e da confiança social.

O caso brasileiro evidenciou que os principais desafios para a ampliação da profundidade estratégica nacional não se encontram apenas na infraestrutura física, mas principalmente na redução da dependência tecnológica externa e no fortalecimento da resiliência cognitiva.

Os resultados obtidos também permitiram formular a Lei da Profundidade Estratégica Informacional:

A capacidade de sobrevivência estratégica de um Estado na Era Informacional é diretamente proporcional ao grau de profundidade existente em suas camadas física, lógica e cognitiva e inversamente proporcional à sua dependência tecnológica externa.

Essa proposição sintetiza o núcleo explicativo da teoria e oferece um princípio geral para a compreensão da soberania e da competição estratégica no século XXI.

Em termos de contribuição científica, a pesquisa produziu cinco avanços principais.

Primeiramente, ampliou o conceito clássico de profundidade estratégica para o contexto da Era Informacional. Em segundo lugar, integrou as literaturas de Geopolítica, Resiliência Nacional, Poder Cibernético e Soberania Cibernética em uma única estrutura analítica. Em terceiro lugar, incorporou a dimensão cognitiva como componente central da sobrevivência estratégica. Em quarto lugar, introduziu a dependência tecnológica como variável explicativa da vulnerabilidade estatal.

Por fim, desenvolveu um índice destinado à operacionalização empírica da teoria.

Naturalmente, a pesquisa apresenta limitações.

A principal delas refere-se ao caráter inicial da formulação proposta.

A TPEC necessita ser submetida a testes empíricos adicionais envolvendo diferentes contextos nacionais e séries históricas mais amplas.

Da mesma forma, o IPEC deverá ser refinado mediante a utilização de bases de dados internacionais e técnicas estatísticas avançadas.

Essas limitações, entretanto, não reduzem a relevância da contribuição apresentada.

Ao contrário, evidenciam a existência de uma agenda de pesquisa ampla e promissora.

Estudos futuros poderão desenvolver análises comparativas envolvendo um número maior de países, investigar a relação entre profundidade estratégica informacional e poder nacional, aperfeiçoar os indicadores do IPEC e examinar os impactos de tecnologias emergentes, como inteligência artificial avançada, computação quântica e sistemas autônomos.

Conclui-se, portanto, que a Teoria da Profundidade Estratégica Cibernética oferece uma nova estrutura conceitual para compreender os desafios da soberania e da sobrevivência estatal na Era Informacional.

Assim como a Geopolítica clássica buscou explicar a relação entre poder e território na Era Industrial, a TPEC procura explicar a relação entre poder, informação e resiliência no século XXI.

Em um mundo cada vez mais dependente de sistemas digitais, fluxos informacionais e tecnologias críticas, a profundidade estratégica informacional tende a tornar-se um dos principais determinantes da autonomia, da segurança e do poder dos Estados.

Nesse sentido, a TPEC apresenta-se não apenas como uma proposta teórica, mas como um novo paradigma analítico para os Estudos

REFERÊNCIAS BIBLIOGRÁFICAS

BETZ, David J.; STEVENS, Tim. **Cyberspace and the state: toward a strategy for cyber-power.** London: Routledge, 2011.

BOIN, Arjen; COMFORT, Louise K.; DEMCHAK, Chris C. **Designing resilience: preparing for extreme events.** Pittsburgh: University of Pittsburgh Press, 2010.

BUZAN, Barry. **People, states and fear: an agenda for international security studies in the post-Cold War** era. 2. ed. Boulder: Lynne Rienner Publishers, 1991.

CASTELLS, Manuel. **The rise of the network society.** 2. ed. Oxford: Wiley-Blackwell, 2010.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber war: the next threat to national security and what to do about it.** New York: HarperCollins, 2010.

CAVELTY, Myriam Dunn. **Cyber-security and threat politics: US efforts to secure the information age.** London: Routledge, 2008.

DEIBERT, Ronald J. **Tracking the emerging armature of cyberspace governance.** Studies in Political Economy, v. 68, n. 1, p. 129-148, 2002.

DENARDIS, Laura. **The global war for internet governance.** New Haven: Yale University Press, 2014.

FLORIDI, Luciano. **The fourth revolution: how the infosphere is reshaping human reality.** Oxford: Oxford University Press, 2014.

GARTZKE, Erik. **The myth of cyberwar: bringing war in cyberspace back down to earth.** International Security, v. 38, n. 2, p. 41-73, 2013.

GRAY, Colin S. **Modern strategy.** Oxford: Oxford University Press, 1999.

KEOHANE, Robert O.; NYE, Joseph S. **Power and interdependence.** 4. ed. New York: Longman, 2012.

KELLO, Lucas. **The virtual weapon and international order.** New Haven: Yale University Press, 2017.

KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. (org.). **Cyberpower and national security.** Washington, DC: National Defense University Press, 2009.

KUEHL, Daniel T. **From cyberspace to cyberpower: defining the problem.** In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. (org.). **Cyberpower and national security.** Washington, DC: **National Defense University Press,** 2009. p. 24-42.

LIBICKI, Martin C**. Cyberdeterrence and cyberwar.** Santa Monica: RAND Corporation, 2009.

LINKOV, Igor; PALMER, Benjamin; KEISLER, Jeffrey. **Fostering resilience to extreme events within infrastructure systems.** Berlin: Springer, 2017.

MACKINDER, Halford J. **Democratic ideals and reality.** Washington, DC: National Defense University Press, 1996.

MAHAN, Alfred Thayer. **The influence of sea power upon history,** 1660-1783. New York: Dover Publications, 1987.

MEARSHEIMER, John J. **The tragedy of great power politics.** New York: W. W. Norton, 2001.

MORENO JUNIOR, Wanderlino. **O jogo do poder no espaço cibernético.** Tagora, 2024.

MORENO JUNIOR, Wanderlino. **Soberania cibernética: Estado, poder e governança na Era Informacional.** São Paulo: Dialética, 2026.

MUELLER, Milton. **Will the internet fragment? Sovereignty, globalization and cyberspace.** Cambridge: Polity Press, 2017.

NYE, Joseph S. **Cyber power.** Cambridge: Harvard Kennedy School, 2010.

NYE, Joseph S. **The future of power.** New York: PublicAffairs, 2011.

OECD. **Digital economy outlook** 2024. Paris: OECD Publishing, 2024.

RID, Thomas. **Cyber war will not take place.** London: Hurst, 2013.

SIMON, Herbert A. **Administrative behavior: a study of decision-making processes in administrative organizations.** 4. ed. New York: Free Press, 1997.

SINGER, Peter W.; FRIEDMAN, Allan. **Cybersecurity and cyberwar: what everyone needs to know.** Oxford: Oxford University Press, 2014.

SPYKMAN, Nicholas J. **America's strategy in world politics: the United States and the balance of power.** New York: Routledge, 2007.

STANFORD UNIVERSITY. **AI Index Report 2025.** Stanford: Institute for Human-Centered Artificial Intelligence, 2025.

TAINTER, Joseph A. **The collapse of complex societies.** Cambridge: Cambridge University Press, 1988.

UNITED NATIONS. **E-government survey 2024: accelerating digital transformation for sustainable development.** New York: United Nations, 2024.

WALTZ, Kenneth N. **Theory of international politics.** Reading: Addison-Wesley, 1979.

WÆVER, Ole. **Securitization and desecuritization.** In: LIPSCHUTZ, Ronnie D. (org.). On security. New York: Columbia University Press, 1995. p. 46-86.

WENDT, Alexander. **Social theory of international politics.** Cambridge: Cambridge University Press, 1999.

WILDAVSKY, Aaron. Searching for safety. New Brunswick: Transaction Publishers, 1988.

WIPO. **Global Innovation Index 2025.** Geneva: **World Intellectual Property Organization, 2025.**

WORLD ECONOMIC FORUM. **Global risks report 2025.** Geneva: World Economic Forum, 2025.

---

[1] Adido de Defesa do Brasil em Angola. E-mail: acesse o artigo original para visualizar o e-mail. ORCID: 0009-0003-9496-175X